IPVM
2020
IP NETWORKING
INTRO

Table Of Contents

Bandwidth Fundamentals

Bandwidth is the most fundamental element of computer networking for video surveillance systems. Because video surveillance can consume an immense amount of bandwidth and because variations in bandwidth load of surveillance cameras can be so significant, understanding bandwidth for video surveillance is critical.

We break down each of the following:

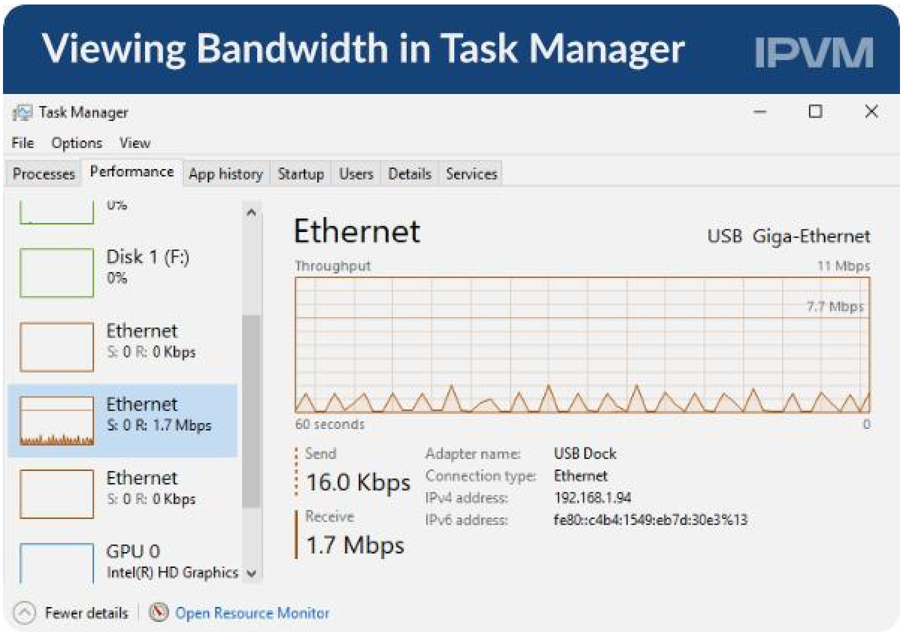
- Measuring Bandwidth
- Bits vs Bytes
- Kilo vs Mega vs Giga
- Bit Rates
- Compression and Bandwidth
- Bandwidth Per Camera
- Constant vs Variable Bit Rates (CBR vs VBR)
- Drivers of Camera Bandwidth Consumption
- Practical Examples of Camera Bandwidth
- Bandwidth Variance Over Time
- Bandwidth and Recorder Placement
- Client Viewing: Multi-Streaming and Transcoding
- Symmetric vs Asymmetric Networks

- Network Bandwidth Capacities
- LAN vs WAN
- Sizing Networks for Video Surveillance
- **Quiz Yourself**: 10 Question Quiz to measure your knowledge on bandwidth for video networks

Measuring Bandwidth

Bandwidth is typically measured in bits (e.g., 100Kb/s, 1Mb/s, 1000Mb/s, etc.). A bit is the most fundamental unit of bandwidth and storage.

You should be comfortable measuring the bandwidth, in bits, on your computer. On a PC, this can be done by opening up the task manager as shown below:



Viewing Bandwidth in Task Manager

Send
16.0 Kbps

Receive
1.7 Mbps

Adapter name: USB Dock
Connection type: Ethernet
IPv4 address: 192.168.1.94
IPv6 address: fe80::c4b4:1549:eb7d:30e3%13

On your computer, it typically shows bandwidth being received by and bandwidth being sent out from your computer (i.e., when you watch a YouTube video you are receiving bandwidth, when you send an email you are transmitting bandwidth). These are also known as download and upload speeds respectively.

Bits vs Bytes

In video surveillance, bandwidth is typically measured in bits but sometimes measured in bytes, causing confusion. 8 bits equals 1 byte, so someone saying 40 Megabits per second and another person saying 5 Megabytes per second mean the same thing but is easy to misunderstand or mishear.

Note: Click here to view the animation on IPVM.

Bits and bytes both use the same letter for shorthand reference. The only difference is that bits uses a lower case ‘b’ and bytes uses an upper case ‘B’. You can remember this by recalling that bytes are ‘bigger’ than bits. We see people confuse this often because at a glance they look similar. For example, 100Kb/s and 100KB/s, the latter is 8x greater than the former.

We recommend you use bits when describing video surveillance bandwidth but beware that some people, often from the server / storage side, will use bytes. Because of this, be alert and ask for confirmation if there is any unclarity (i.e., “Sorry did you say X bits or bytes”).

Kilo vs Mega vs Giga

It takes a lot of bits (or bytes) to send video. In practice, you will never have a video stream of 500b/s or even 500B/s. Video generally needs at least thousands or millions of bits. Aggregated video streams often need billions of bits.

The common expression / prefixes for expressing large amount of bandwidth are:

- Kilobits, is thousands, e.g., 500Kb/s is equal to 500,000b/s. An individual video stream in the kilobits tends to be either low resolution or low frame or high compression (or all of the above).
- Megabits is millions, e.g., 5Mb/s is equal to 5,000,000b/s. An individual HD / MP video stream tends to be in the single digit megabits (e.g., 2Mb/s or 4Mb/s or 8Mb/s are fairly common ranges). More than 10Mb/s for an individual video stream is less common (the most typical case is from using the less bandwidth efficient MJPEG codec). However, a 100 cameras being streamed at the same time can routinely require 200Mb/s or 400Mb/s, etc.
- Gigabits is billions, e.g., 5Gb/s is equal to 5,000,000,000b/s. One rarely needs more than a gigabit of bandwidth for video surveillance unless one has a very large-scale surveillance system backhauling all video to a central site.

Bit Rates

Bandwidth is like vehicle speed. It is a rate over time. So just like you might say you were driving 60mph (or 96kph), you could say the bandwidth of a camera is 600Kb/s, i.e., that 600 kilobits were transmitted in a second. If you say the bandwidth of your camera is 600Kb or 600KB, not only will you be wrong, you will look incompetent.

Bit rates are always expressed as data (bits or bytes) over a second. Per minute or hour are not applicable, primarily because networking equipment is rated as what the device can handle per second.

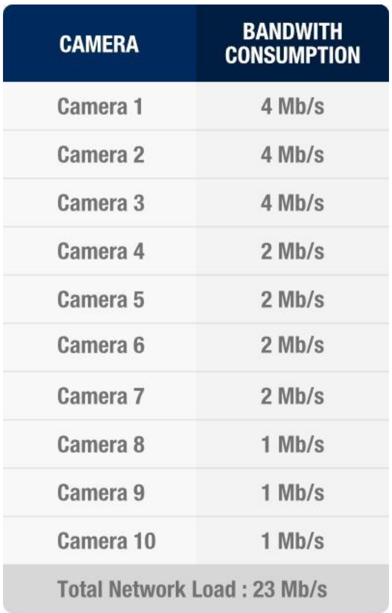
Compression and Bandwidth

Essentially all video surveillance that is sent on an IP network is compressed. Surveillance cameras can produce uncompressed video (e.g., analog) but that is almost always compressed before sending over a network. It is theoretically possible to send uncompressed surveillance video over a network but the immense bit rate of even a single stream (1,000Mb/s+) makes it impractical and unjustifiable for almost all.

Bandwidth Per Camera

Bandwidth is typically measured per camera and the amount of bandwidth each camera needs can vary significantly.

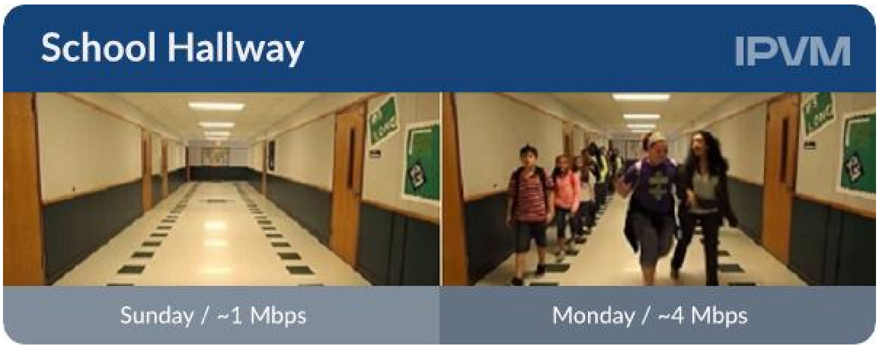
One can and should sum / add up the bandwidth needs of each camera on a network to determine total load. For example, if you have 10 cameras on a network and 3 of them use 4Mb/s, 4 of them use 2Mb/s and 3 of them use 1Mb/s, the total load on the network for those 10 cameras would be 23Mb/s.



CAMERA	BANDWITH CONSUMPTION
Camera 1	4 Mb/s
Camera 2	4 Mb/s
Camera 3	4 Mb/s
Camera 4	2 Mb/s
Camera 5	2 Mb/s
Camera 6	2 Mb/s
Camera 7	2 Mb/s
Camera 8	1 Mb/s
Camera 9	1 Mb/s
Camera 10	1 Mb/s
Total Network Load : 23 Mb/s	

Constant vs Variable vs Max Bit Rates (CBR vs VBR vs MBR)

The amount of bandwidth a camera needs at any given time to maintain a specific quality level varies over time, sometimes substantially. For example, a camera might need 1Mb/s for an empty school hallway on a Sunday afternoon but might need 4Mb/s for that same spot come Monday morning.



There are three ways to deal with this:

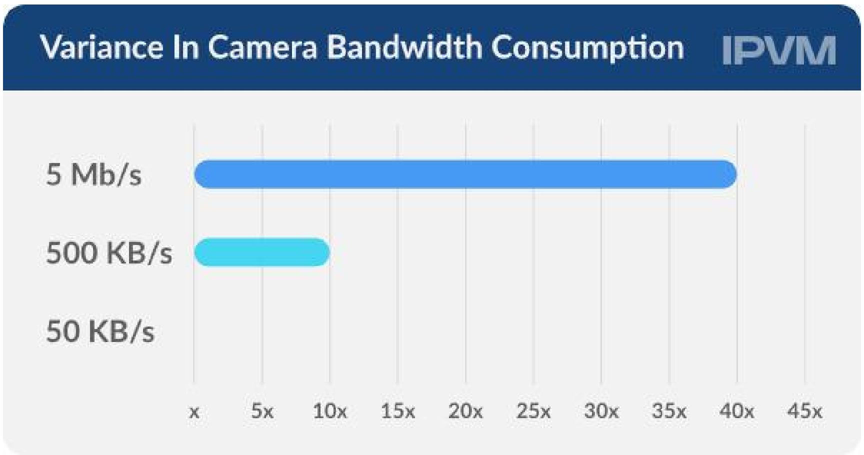
- Variable bit rate (VBR), where the bit rate changes to keep compression at a set level regardless of activity.
- Maximum bit rate (MBR), also called VBR with a cap, where the bit rate changes but no more than a user defined maximum.
- Constant bit rates (CBR), where the bit rate of the camera does not change even if the scene does.

Knowing what type of bit rate control a camera uses is critical, because it impacts bandwidth load significantly. For more, see: CBR vs VBR vs MBR: Surveillance Streaming.

Drivers of Camera Bandwidth Consumption

There is no set standard or even typical camera bandwidth consumption. Using a vehicle example, on a US highway, you can reasonably estimate that almost all cars will drive between 55mph and 85mph.

For video surveillance, some video feeds are as low as 50Kb/s (.05Mb/s) and others are routinely 300 times higher at (15000Kb/s) 15Mb/s.



Here are a few common drivers of camera bandwidth consumption:

- Resolution: everything else equal, the greater the resolution, the greater the bandwidth
- Frame rate: everything else equal, the greater the frame rate, the greater the bandwidth
- Scene complexity: The more activity in the scene (lots of cars and people moving vs no on in the scene), the greater the bandwidth needed.
- Low light: Night time often, but not always, requires more bandwidth due to noise from cameras. See: Testing Bandwidth vs Low Light.

- Model variations: Some models depending on imager or processing can consume far more or less bandwidth.
- Smart Codecs: This is relatively new (developed over the past couple of years), but some cameras even using the same H.264 codec, can intelligently adapt compression for great bandwidth reduction. See: Smart CODEC Guide

Practical Examples of Camera Bandwidth

The following list is an excerpt from IPVM tests of actual bandwidth recording for a variety of cameras:

- CIF 5FPS Office: 50 KB/s
- 720P 10FPS Conference Room: 0.5 Mb/s
- 720P 30FPS Intersection: 4 Mb/s
- 1080P 10FPS Conference Room: 2 Mb/s
- 1080P 30FPS IR On Intersection: 8 Mb/s
- 5MP 15FPs Panoramic Office: 4.5 Mb/s
- 4K 30FPS Intersection: 7 Mb/s
- 4K 10 FPS Night Outdoors: 32 Mb/s

Bandwidth and Recorder Placement

Video surveillance consumes network bandwidth in one of the following 2 typical scenarios:

- Camera / encoder to recorder: Video is generally generated in different devices than they are recorded (e.g., a camera generates the video, a DVR / NVR / VMS server records it). In between, the video needs to be transmitted. If it goes over an IP network (e.g., IP cameras to NVR / VMS), bandwidth is required.

- Recorder to client: Statistically, a very low percentage of video is watched by humans. Often, where the person is watching is on a different device on an IP network than the recorder. For example, the recorder might be in a rack in an IT closet but the viewer (i.e., client) is on a laptop, mobile phone or a monitoring station.

Because of this design, the overwhelming majority of bandwidth needed in surveillance systems is dictated by (1) camera type and (2) the relative placement of cameras and recorders.

In terms of camera type, non IP cameras (NTSC / PAL analog, Analog HD, HD SDI) typically do not consume network bandwidth unless video is being sent to clients as each camera has a cable directly connected to a recorder.

For all camera types, the relative physical placement of the recorder near the camera significantly impacts bandwidth needs. For example, imagine 1000 cameras, with 100 cameras each at 10 buildings on a campus. If each building has a recorder, the peak bandwidth requirements will be ~90% lower than if there is only a single site for recording (i.e., each building recording its own might only need ~200Mb/s network connection compared to ~2Gb/s if they are all being sent back to one building). There are pros and cons to each approach but knowing where you will place recorders has a major impact.

LAN vs WAN

The local area network (LAN) and the wide area network (WAN) are two common acronyms in networking. LAN, as the name implies, refers to networks that are local to a building or campus. By contrast, the WAN, are networks that connect 'widely' across cities, states, countries, etc.

Relatively speaking, bandwidth is cheaper and easier on LANs than WANs.

Network Bandwidth Capacities

In LANs, the three most common network bandwidth capacities are:

- 100Mb/s
- 1,000Mb/s (1 Gig)
- 10,000Mb/s (10 Gig)

In particular, 100Mb/s and 1,000Mb/s connections are quite ordinary for modern networks. For more, see the IP Network Hardware for Surveillance Guide.

Lower than 100Mb/s networks in LANs are relics of the past. They may exist from networks installed many years ago but no one installs LAN networks under 100Mb/s today.

WANs can deliver the same or more bandwidth as the LAN but the costs tend to be significantly higher (in the order of 10 or 100x more expensive per bit) because these networks need to run great distances and across many obstacles. While one certainly could secure a 1 Gig WAN connection, the likelihood that one would do this for surveillance is very low, given the cost this would typically incur.

Symmetric vs Asymmetric Bandwidth

Many WAN networks / connections have asymmetric bandwidth, a problem for remote monitoring or recording of video.

Symmetric bandwidth means the bandwidth is the same ‘up’ and ‘down’, i.e., a link can send the same amount of bandwidth as it can receive (100Mb/s up and 100Mb/s down is a classic example).

Asymmetric bandwidth means the bandwidth up and down are not the same. Specifically, the bandwidth ‘up’ is frequently much lower than the bandwidth ‘down’. This is common in homes and remote offices. These asymetric connections provide sufficient downstream speeds while only providing ~10% of those speeds for upload. The downstream bandwidth might be 10Mb/s or 25Mb/s but the upstream might only be 500 Kb/s or 2Mb/s. In this example, if someone at home wanted to stream a movie (send it downstream from the cloud / Internet), it would not be a problem but if they wanted to upload a movie (or HD surveillance feed), it would be a problem.

The most common asymmetric bandwidth WAN networks are:

- Cable Modem
- DSL
- Satellite

The main exceptions, those that offer symmetrical bandwidth commonplace, are:

- Telecommunication / telephony networks (e.g., T1s, T3s) but these are fairly expensive and relatively low bit rate (e.g., respectively 1.5Mb/s and 45Mb/s)
- Fiber to the Home (FTTH) / Business (FTTB) are much less expensive than telephony networks and routinely offer 100Mb/s connections. The main limitation is access to such networks. While increasing over

the past decade, they tend to be limited to densely populated urban areas.

Sizing Networks for Video Surveillance

Putting this information together, to size a network for video surveillance, you will need to know:

- How much bandwidth each camera consumes, recognizing that wide variations can exist
- How close (or far) the recorder is going to be placed to the cameras connected to it, presuming they need an IP network
- What the bandwidth of those network connections are and what pre-existing load those networks must also support.

For more, see: How to Calculate Surveillance Storage / Bandwidth

Quiz Yourself

See how much you know: Take the 10 Question Bandwidth for Video Networks Quiz

Network Addressing

The goal of this guide is to explain addressing devices on IP networks, focusing on how IP cameras and recorders are used in those networks. For even more IP networking basics, see our IP Video 101 Training.

We cover the following topics and their impact on surveillance/security networks:

- MAC Addresses
- Multiple MACs Possible
- Manufacturer OUIs
- OEM Devices
- IP Addresses
- Address Conflicts
- Subnet Mask
- Subnetting Large Deployments
- Default Gateways
- IPv4 vs IPv6 Formats
- Video and IP Addresses
- Dynamic vs. Static Addresses

- Public vs Private Addresses
- Zero Config
- Network Classes
- Loopback / localhost
- Test Yourself

MAC Addresses

All network devices (PCs, servers, cameras, switches, etc.) have a fixed address, called a MAC address (Media Access Control), a unique 12 character identifier, such as:

AC:CC:8E:0C:B5:F4

Since MAC addresses are issued at the factory and do not change, they are often used for identifying devices on a network even if the IP address is unknown or has changed.

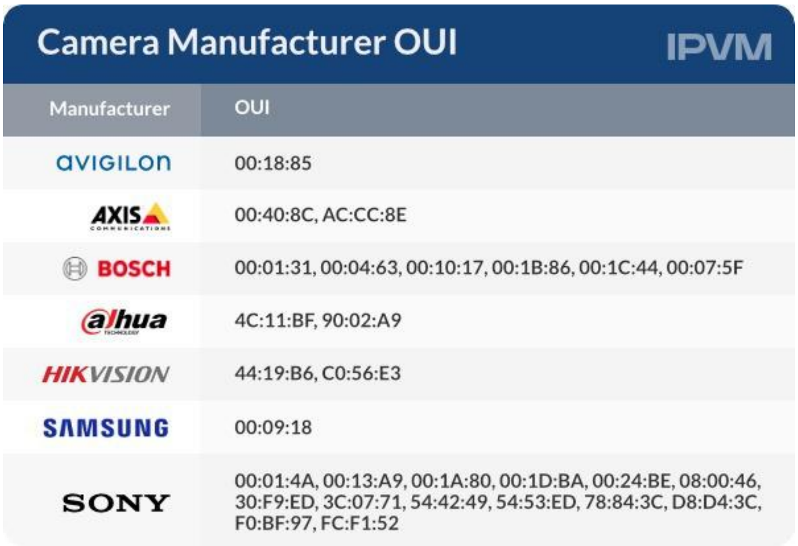
Multiple Network Interface = Multiple MACs

If a device has multiple network interfaces, it may have more than one single MAC address as the MAC is associated with a device's network interfaces, not the general device. In the case of cameras with multiple network connections (e.g., a camera with both a wired ethernet port and an integrated wireless radio), the device would have multiple MAC addresses.

Since the vast majority of cameras include only a single ethernet port, the MAC address could be/is often indirectly used to describe the entire camera.

Organizationally Unique Identifier

The first six digits of a MAC are called the OUI, and each manufacturer is assigned one or more unique identifiers. For example, these are the OUIs of some common cameras manufacturers:



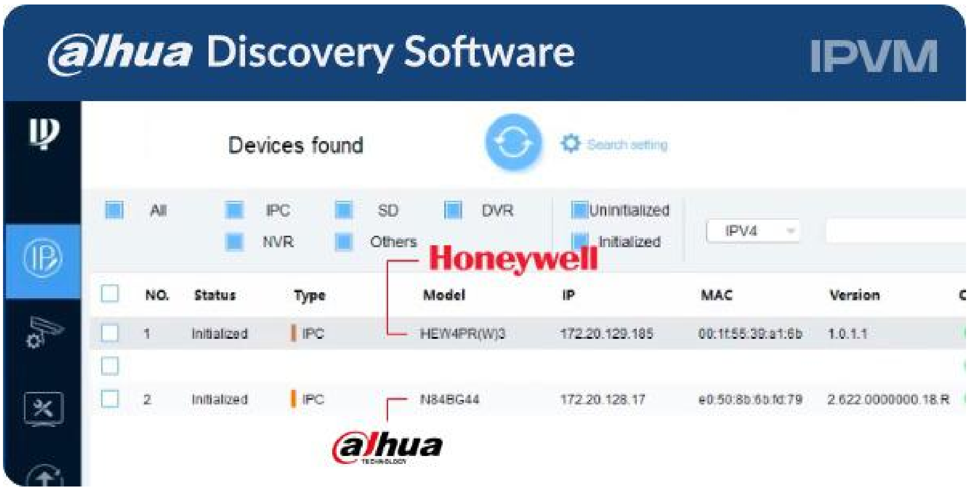
Camera Manufacturer OUI IPVM

Manufacturer	OUI
avigilon	00:18:85
AXIS COMMUNICATIONS	00:40:8C, AC:CC:8E
BOSCH	00:01:31, 00:04:63, 00:10:17, 00:1B:86, 00:1C:44, 00:07:5F
alhua TECHNOLOGY	4C:11:BF, 90:02:A9
HIKVISION	44:19:B6, C0:56:E3
SAMSUNG	00:09:18
SONY	00:01:4A, 00:13:A9, 00:1A:80, 00:1D:BA, 00:24:BE, 08:00:46, 30:F9:ED, 3C:07:71, 54:42:49, 54:53:ED, 78:84:3C, D8:D4:3C, F0:BF:97, FC:F1:52

In the case of manufacturers such as Sony, which are part of a larger conglomerate, it is difficult to know which of these OUIs is used specifically for security without scanning devices, as they are listed simply as "Sony Corporation" in OUI lookups. Here is an OUI to manufacturer lookup engine that lets you put in any manufacturer (IP cameras, DVRs, PCs, etc.) and find their OUIs.

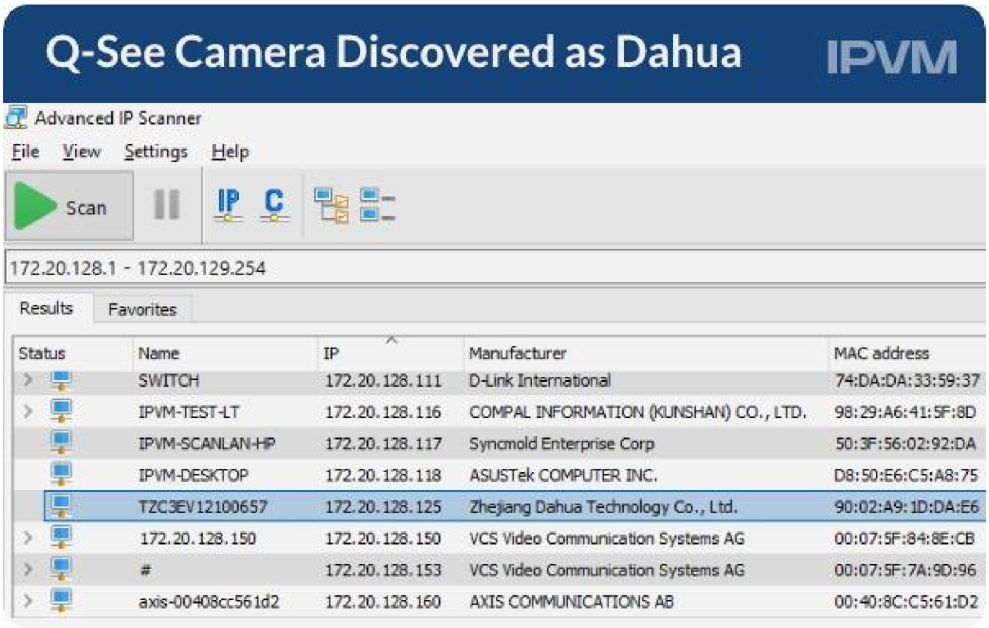
OEM Devices

In cases where manufacturers OEM their devices from another, which OUI is used depends on manufacturing agreements. For example, checking the MAC address of a Honeywell camera manufactured by Dahua (00:1f:55), it is listed as Honeywell, however since they are using basically the same firmware it is discovered as a Dahua camera within Dahua's device discovery software:



□	NO.	Status	Type	Model	IP	MAC	Version
□	1	Initialized	IPC	HEW4PR(W)3	172.20.129.185	00:1f:55:39:a1:6b	1.0.1.1
□							
□	2	Initialized	IPC	N84BG44	172.20.128.17	e0:50:8b:6b:fd:79	2.622.0000000.18.R

Others, however, show the OUI of the original manufacturer relabeling the camera. Below a Q-See brand camera is discovered at Dahua.



172.20.128.1 - 172.20.129.254

Status	Name	IP	Manufacturer	MAC address
>	SWITCH	172.20.128.111	D-Link International	74:DA:DA:33:59:37
>	IPVM-TEST-LT	172.20.128.116	COMPAL INFORMATION (KUNSHAN) CO., LTD.	98:29:A6:41:5F:8D
	IPVM-SCANLAN-HP	172.20.128.117	Syncmold Enterprise Corp	50:3F:56:02:92:DA
	IPVM-DESKTOP	172.20.128.118	ASUSTek COMPUTER INC.	D8:50:E6:C5:A8:75
	TZC3EV12100657	172.20.128.125	Zhejiang Dahua Technology Co., Ltd.	90:02:A9:1D:DA:E6
>	172.20.128.150	172.20.128.150	VCS Video Communication Systems AG	00:07:5F:84:8E:CB
>	#	172.20.128.153	VCS Video Communication Systems AG	00:07:5F:7A:9D:96
>	axis-00408cc561d2	172.20.128.160	AXIS COMMUNICATIONS AB	00:40:8C:C5:61:D2

IP Addresses Defined

In video surveillance, many components are IP addressed, including IP cameras, encoders, recorders, access control panels, and more. The IP address of a camera is used to add it to a VMS or NVR, while client software connects to the VMS or NVR typically via its IP address.

An IP address (IPv4 specifically) consists of four parts (called octets because they contain 8 bits of data) ranging in value from 0-255, separated by periods, such as:

192.168.1.49

The IP address is divided into a network address (192.168.1 in the example above) and a host address (.49 in this case). On a single LAN, the network address is typically the same for all devices, while the host address differs. So 192.168.1.49, 192.168.1.50, and 192.168.1.51 all reflect different devices on the same network.

Analog vs IP Cameras IP Addressing

Analog cameras (whether SD or HD), by definition of being analog, do not have or need IP addresses since they have no network interface. However, analog cameras are generally connected to recorders or encoders that do have network interfaces and therefore use IP addresses.

IP Address Conflicts

If more than one device attempts to use the same IP address, generally neither will be able to connect to the network. On PCs, the user is typically notified that a device has connected and is causing an IP address conflict. However, if two cameras share the same address, errors will typically not be generated, but cameras may randomly go offline or not stream video to a recorder, leading to wasted troubleshooting time.

Note that some manufacturers ship their cameras with a hardcoded default IP address. Plugging more than one into the network at a time may cause address conflicts, so these cameras must be connected one at a time and re-addressed. Installers should check if their chosen manufacturer(s) use default IP addresses and plan initial setup accordingly. An IP Scanner may save you time and frustration.

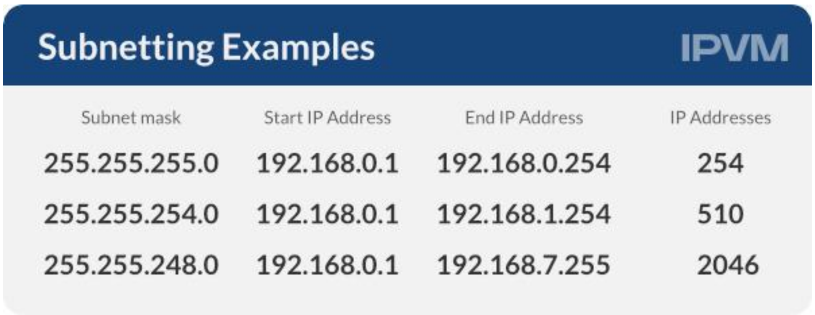
Subnet Mask / Subnetting

Subnet masks are an advanced topic in IP addressing, outside the scope of this report. Essentially, a subnet mask determines which parts of an IP address reflect the "network" vs. the "host." In practice, the vast majority of networks, surveillance included, use default subnet masks for the IP address class (discussed below), most commonly 255.255.255.0. In class B networks, e.g., 172.20.x.x), the default subnet mask is 255.255.0.0.

Subnets In Large Deployments

For larger camera networks which require over 255 device addresses, subnet masks are most often used to expand the network to an additional subnet or subnets. This is done by changing the last octet of the mask. For every bit that is removed, an additional 255 host subnet becomes available.

As a practical example, changing subnet mask from 255.255.255.0 to 255.255.25**4**.0 on a 192.168.0.1 network allows users to expand into the 192.168.1.1 network without using a router, a total of 510 hosts instead of 255, effectively doubling available IP addresses. Changing the mask to 255.255.248.0 expands this further to 2046 IPs (192.168.0.1-192.168.7.254).



Subnetting Examples

Subnet mask	Start IP Address	End IP Address	IP Addresses
255.255.255.0	192.168.0.1	192.168.0.254	254
255.255.254.0	192.168.0.1	192.168.1.254	510
255.255.248.0	192.168.0.1	192.168.7.255	2046

To see how subnet masks impact available addresses, users may refer to commonly available subnet calculators.

For those interested in more information on subnetting, please see our report on Subnetting For Video Surveillance.

Default Gateways

Generally, and typically in video surveillance, the term "default gateway" is synonymous with routers. IP cameras and DVRs, like PCs, have fields to enter the address of the default gateway. In practice, this means the address of the router — the "gateway" to the internet.

The default gateway is needed for computers on other networks to access the IP video surveillance equipment. For example, users at a remote site or on their phones would typically not be able to connect to an IP camera or recorder that does not have a default gateway set. Sometimes, in security applications, not entering in a default gateway is done on purpose, to block any access to the system.

IPv4 vs. IPv6

Because the use of the internet has expanded over time, concerns about the number of addresses available using IPv4 format arose (called address exhaustion), lead to the development of an expanded address format, IPv6.

Unlike IPv4, which uses 32 bits (8x4) for each address, IPv6 uses 16 octets (128 bits total), displayed in hexadecimal (0-9 + A-F). Each group separated by colons represents two octets. For example:

FA80:4322:0000:0000:0202:B3EF:FE1E:8329

This increase in address size results in approximately 34 undecillion addresses, a huge increase over the IPv4 limit of about 4.2 billion addresses.

Many networks support either and both formats, and most modern IP cameras can be configured to use either format. Note that the same format should be used throughout.

IPv4 for Surveillance

Despite IPv6's larger address pool, IPv4 continues to be the dominant format used. Especially for private networks, with a finite number of connected devices like a surveillance system, address exhaustion is not a practical problem. IPv4 remains easier to use and administer, and there is little or no reason to use the more complex IPv6 format.

IPv6 Growing For Internet Addresses

Despite its limited use in surveillance networks, Google reports that IPv6 usage among their users has jumped from ~10% in 2016 to ~20% so far in 2018. This comes after taking 20 years (from IPv6's RFC adoption in 1996 until 2016) to reach 10%.

This growing adoption may increase use in internal networks, but IPv6 is likely to remain limited to the public Internet for some time.

Static vs. Dynamic Addressing

Devices may be set with either a static (does not change over time) or dynamic (changes periodically based on lease time) IP address. Because cameras and NVRs are typically fixed devices and configured to communicate via IP address, giving them dynamic addresses may cause issues when the IP changes, forcing users to reconfigure devices. Therefore, all devices in security systems are typically manually assigned static addresses. Using dynamic addresses for devices that need to be found via their IP address is comparable to trying to deliver postal to homes in a town where the houses are renumbered and the streets are renamed periodically.

However, there are some cases in which dynamic addresses may be used.

- When setting up a new surveillance network, a DHCP (dynamic host configuration protocol) server is often used to temporarily assign IP addresses to devices so they may be reached for configuration. for example, a new camera connected to the network receives an address from the server, which the installer users to perform initial configuration and assign a permanent address.
- Some less crucial devices, such as client PCs and tablets may be dynamically addressed. Since these devices are typically used only periodically, and generally do not need to be reached for configuration or connected to a VMS by IP address as cameras are, assigning them a dynamic address is often sufficient.

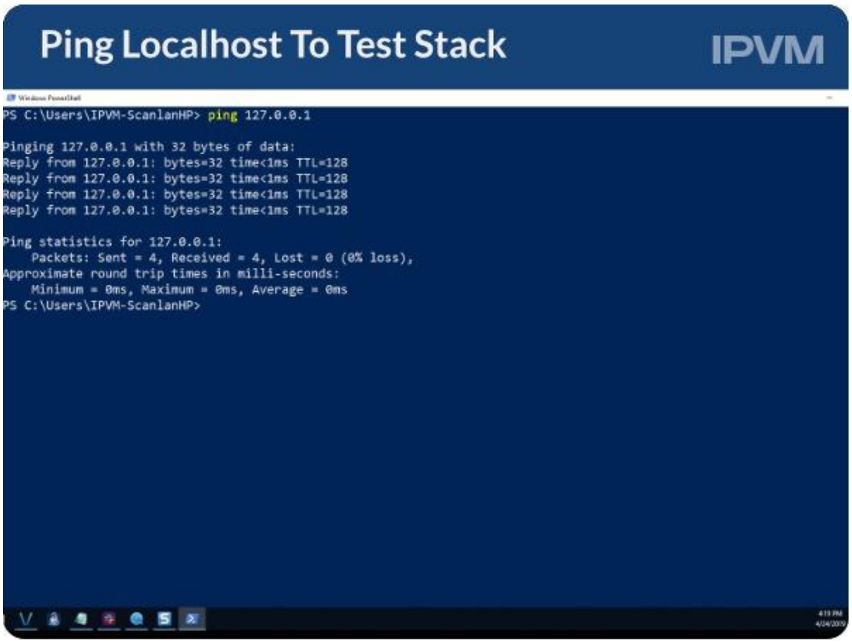
For more detail on why static addressing is best practice for IP video systems, read our Dynamic vs. Static IP Addresses post.

Zero-Configuration

There is a subset of dynamic addresses available in use by zero-configuration, commonly called zeroconf, which allows devices to use a dynamic address without a DHCP server in place. In surveillance, the most common example of this is initial setup of IP cameras. Connecting a laptop directly to a camera, with both devices set to use dynamic addressing, they will both be automatically addressed to an address beginning with 169.254. This allows initial configuration to be performed and the IP address changed without needing a DHCP server (note that many, but not all, current cameras support this).

Loopback / localhost

The address 127.0.0.1 is the localhost / loopback address and serves two purposes. As the loopback address it is used for testing the TCP/IP protocol stack. If a machine has network connectivity problems, it is way to test that the NIC and protocol are functioning correctly as shown below:



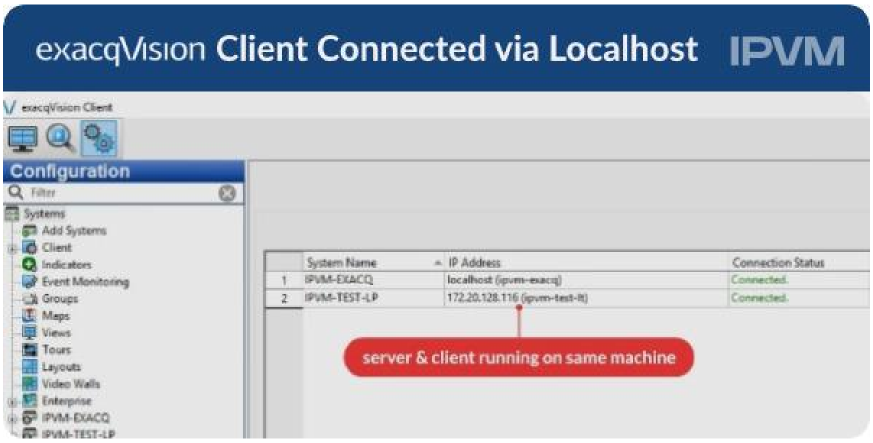
Ping Localhost To Test Stack

```
PS C:\Users\IPVM-ScanlanHP> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\IPVM-ScanlanHP>
```

When used as the localhost, it lets system know that the target is the same as the host. This is commonly used when a client is running on the same machine as a server and for web applications. The screenshot below shows a machine running Exacqvision server and the client on the same machine. The client connects using localhost.

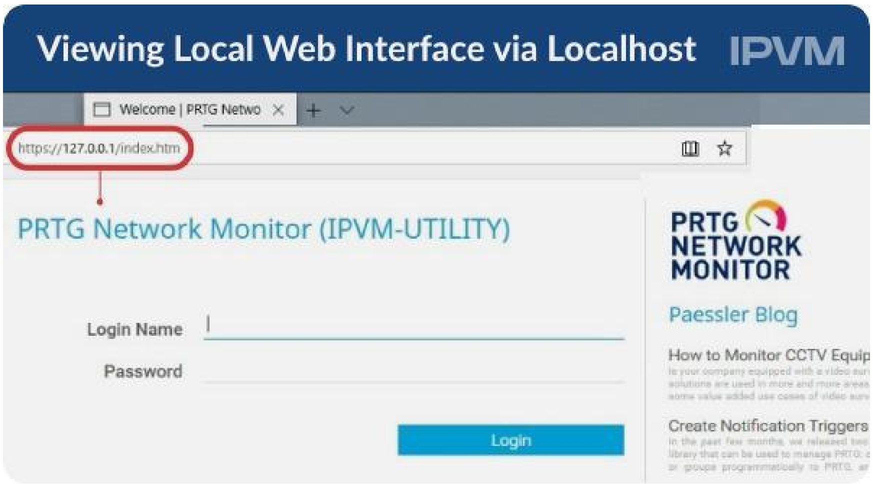


exacqVision Client Connected via Localhost IPVM

	System Name	IP Address	Connection Status
1	IPVM-EXACQ	localhost (ipvm-exacq)	Connected.
2	IPVM-TEST-LP	172.20.128.116 (ipvm-test-lt)	Connected.

server & client running on same machine

Below is an image of machine running PRTG, where entering 127.0.0.1 into a browser on that machine brings us to the web interface for PRTG.



Viewing Local Web Interface via Localhost IPVM

https://127.0.0.1/index.htm

PRTG Network Monitor (IPVM-UTILITY)

Login Name

Password

Network Classes

In general, the relationship between potential unique addresses in a network, and total potential number of unique sub-networks supported is a decision well beyond a surveillance system. The three most common network classes are limited as follows:

- Class A: This type supports over 16 million IP addresses per network, but only supports 128 different subnets. (From 0.0.0.0 to 127.255.255.255)
- Class B: The type supports over 65,000 IP addresses per network, and about 16,000 different subnets. (From 128.0.0.0 to 191.255.255.255)
- Class C: This type supports only 256 IP addresses per network, but almost 3 million subnets. (From 192.0.0.0 to 223.255.255.255)

The vast majority of surveillance/security networks use class C addresses, as the number of devices simply does not require other classes.

Private/ Public Networks

Every device on the Internet has an IP address, but not every networked device is on the internet. The difference is the boundary between private vs. public networks. For example, an IP Video network might consist of hundreds or thousands of cameras without a single unit being directly connected to the internet.

Typically only a few tightly controlled devices like routers or firewalls are given a public IP address. However, some recorders or IP cameras may be publicly available (example 1, 2) on the web. This is far more common in consumer/residential and small office use than midsize and enterprise systems, which typically demand tighter security, with organizations' IT department preferring not to open these devices to the internet.

Portions of the "172" and the "192" address ranges are designated for private networks. The remaining addresses are "public," and routable on the global Internet. Private networks can use IP addresses anywhere in the following ranges:

- 192.168.0.0 - 192.168.255.255 (65,536 IP addresses)
- 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)
- 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

In modern systems, IP addresses are associated with subnet masking, which helps regulate traffic within a network at the expense of adding a trivial configuration step. Most surveillance systems are installed on a class C network, as evidenced in our Which Private IP Addresses Do You Use For IP Video? discussion, in which 50% of respondents said they use 192.168.X networks for their installations.

Test Your Knowledge

Take this 10 question quiz now

[Note: This guide was originally published in 2015, but substantially updated in 2018 to reflect IPv4/IPv6 changes, subnet masking information, and more]

Subnetting

We cover reference of subnetting used in security networks, and how it works. We explain how to add or remove IP addresses to your range, borrowing bits, and the role of the subnet mask.

We provide information on:

- How borrowing bits works
- The role of the subnet mask
- Expanding the IP Pool
- Shrinking the IP Pool
- Common use in security

Why Subnet in Video Surveillance

There are a few reasons administrators may want to subnet their security network, reviewed below:

- Running out of addresses
- Network security
- Ease of administration

Running Out Of Addresses, Aka Address Exhaustion

The most common IP address scheme is 192.168.1.x (a class C network) which provides 254 host addresses. However, in even mid-sized surveillance and security systems, such as a school, mall, or other facility, these addresses may be quickly consumed by cameras and NVRs. Further, adding access control may consume an address for each controller. Wireless radios to connect remote cameras consume additional addresses. Dedicated viewing stations will also require addresses, etc.

By simply changing subnet mask by one bit (255.255.255.0 to 255.255.254.0), the network gains an additional 255 addresses which may be used for additional devices. Every bit adds this same amount, so using a mask of 255.255.240 would provide almost 4,000 devices on the subnet.

Network Security

By using different subnets for different logical networks (e.g., surveillance vs. general LAN vs. voice), a device on subnet is prevented from accessing a device on another. It simply cannot find the route to the other host.

Subnetting is also often deployed with VLANs, which we have more information on here.

Ease Of Administration

Employing subnetting allows you to select an IP scheme with a realistic and manageable amount of hosts. When scanning a network or using a discovery tool on a small network it is quicker to scan a smaller network, closer in number to actual in-use devices, rather than scan thousands of unused addresses; e.g.

Scanning 172.20.0.1 - 172.20.255.254 with subnet 255.255.0.0 = 65,534 addresses

Scanning 172.20.0.1 - 172.20.0.30 with subnet 255.255.255.224 = 30 addresses

The network with the classfull subnet mask will take about 2 hours to scan with a discovery tool, like Advanced IP Scanner, while the smaller subnet work will take just minutes.

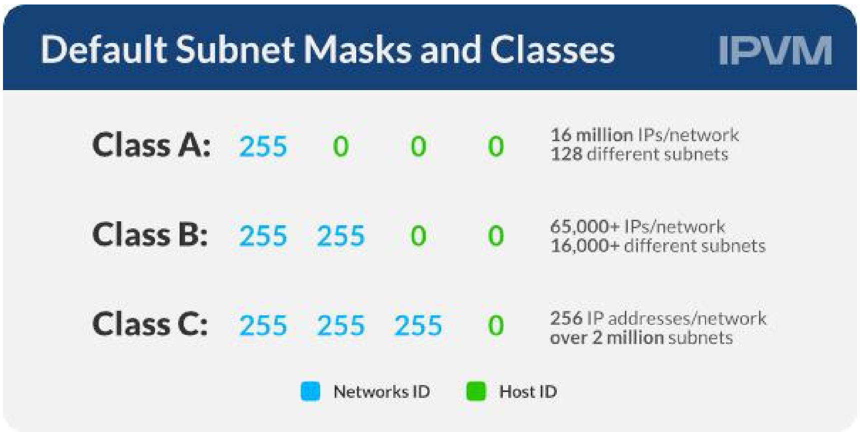
Subnetting Basics

The subnet mask is a companion configuration to the IP address, and determines which parts of an IP address reflect the "network" vs. the "host." In practice, the vast majority of networks, surveillance included, use default subnet masks, also called classfull addressing, for the IP address class, most commonly 255.255.255.0.

[Note, for this guide we are only concerned with private addresses which are broken into 3 classes below.]

Classfull Addresses / Private IP Addresses

Subnetting changes the subnet mask from classfull (Class A = 255.0.0.0, B = 255.255.0.0, C = 255.255.255.0) to classless using borrowed bits to change those values, and in doing so changes the amount of hosts and networks. You can choose to either increase hosts and decrease networks or decrease hosts and increase networks. The graphic below shows the subnet masks for each class and the amount of hosts and networks associated with each.

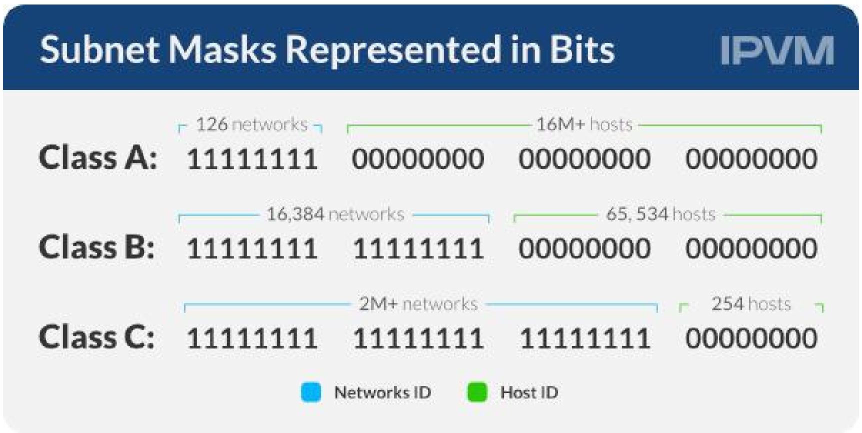


Default Subnet Masks and Classes IPVM

Class A:	255	0	0	0	16 million IPs/network 128 different subnets
Class B:	255	255	0	0	65,000+ IPs/network 16,000+ different subnets
Class C:	255	255	255	0	256 IP addresses/network over 2 million subnets

🟦 Networks ID 🟩 Host ID

The image below shows how bits make up the subnet mask. The network bits are 1's, and 8 bits or 8 1's (11111111) = 255. The host bits are 0's, which 00000000 = 0. The graphic below shows the default subnet mask for each class, and associated bits.



Subnet Masks Represented in Bits IPVM

	126 networks	16M+ hosts		
Class A:	11111111	00000000	00000000	00000000
	16,384 networks		65, 534 hosts	
Class B:	11111111	11111111	00000000	00000000
	2M+ networks			254 hosts
Class C:	11111111	11111111	11111111	00000000

🟦 Networks ID 🟩 Host ID

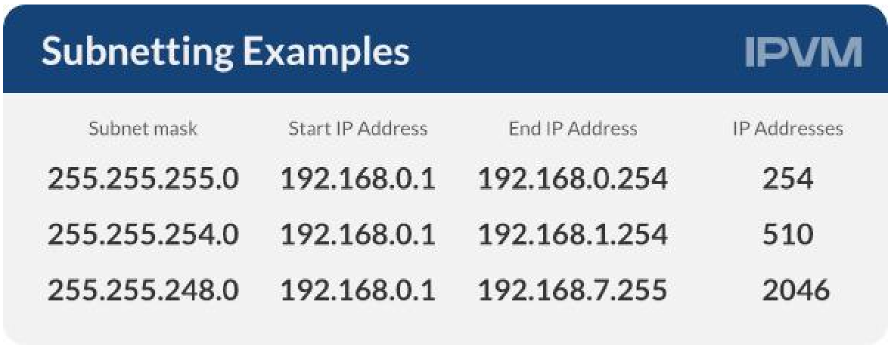
Subnet Mask Determines Networks and Hosts

Deviating from the classfull subnet masks is subnetting, also called classless addressing. The way that this is done is by borrowing bits from the other this is done by changing 1 to 0 or 0 to 1. If more hosts are desired then bits are borrowed from the network portion, and when more networks are desired bits are borrowed from the host portion.

Subnets In Large Deployments

For larger camera networks which require over 255 device addresses, subnet masks are most often used to expand the network to an additional subnet or subnets. This is done by changing the last octet of the mask. For every bit that is removed, an additional 255 host subnet becomes available.

As a practical example, changing subnet mask from 255.255.255.0 to 255.255.25**4**.0 on a 192.168.0.1 network allows users to expand into the 192.168.1.1 network without using a router, a total of 510 hosts instead of 255, effectively doubling available IP addresses. Changing the mask to 255.255.248.0 expands this further to 2,046 IPs (192.168.0.1-192.168.7.254). This is illustrated below.



Subnetting Examples

Subnet mask	Start IP Address	End IP Address	IP Addresses
255.255.255.0	192.168.0.1	192.168.0.254	254
255.255.254.0	192.168.0.1	192.168.1.254	510
255.255.248.0	192.168.0.1	192.168.7.255	2046

To see how subnet masks impact available addresses, users may refer to commonly available subnet calculators.

IP Network Hardware

Video surveillance systems depend on IP networking equipment. We explain the key pieces of equipment and features, explaining where and why they are typically used. The topics covered include:

- Fast / Gigabit / 10 Gigabit Ethernet
- Actual vs. Rated Throughput
- Ethernet Switches
- PoE vs non-PoE Switches
- Managed vs. Unmanaged Switches
- Routers / Default Gateways
- Media Converters - Fiber and Coax
- Ethernet over UTP Extenders
- Ethernet Network Distance
- Wireless
- Network Interface Cards
- Multiple NICs
- Customer Premise Equipment
- Racks and Shelves

Network Speeds

The vast majority of network gear is rated for either 100 Mb/s (Fast Ethernet) or 1,000 Mb/s (Gigabit Ethernet/GbE). These ratings describe throughput capacity, i.e., how much data each port may handle. Other variants, such as 10 or 40 Gigabit Ethernet, are available though generally not used in surveillance.

There are three common speed classes in use in networks today:

- Fast Ethernet: 100 Mb/second
- Gigabit Ethernet: 1,000 Mb/s
- Higher speeds: 10 Gb, 40 Gb, 100 Gb/s

Fast Ethernet

Fast Ethernet (100 Mb/sec) is used for connections to field devices, such as cameras, encoders, and I/O modules. Rarely do these devices support gigabit speeds. Despite multi-megapixel and 4K cameras becoming common (with some including gigabit ports), camera streams are typically 15 Mb/s and below, simply not large enough to warrant the use of Gigabit Ethernet for the bulk of the network.

Gigabit Ethernet

By contrast, Gigabit Ethernet (GbE) devices are rated to handle 10X more data per second than Fast Ethernet devices. GbE devices are generally moderately more expensive (20-30%) than their equivalent Fast Ethernet counterparts. In surveillance, GbE is typically used to connect switches together, as Fast Ethernet is typically not fast enough for these backbones.

Additionally, it may be used to connect servers to storage devices (NAS/SAN).

10+ Gigabit Ethernet

10 GbE and faster speeds are uncommon in surveillance. It is generally used in data center applications connecting large quantities of switches and servers which require more throughput than 1000 Mb/s links can provide. The only likely application for 10 GbE in surveillance is in connecting large quantities of servers to a storage network (SAN), typically only seen in very large systems, such as citywide surveillance.

Faster speeds such as 40 and 100 GbE are very rare, expensive, and unlikely to see use in surveillance in the near future.

Actual Throughput

Total actual throughput capacity of all of these options will be less than the category implies, as other network variables and the switch design itself deduct a portion of bandwidth as overhead. Typically, about 70-80% of rated speed can be expected for actual throughput, meaning 70-80 Mb/s in a Fast Ethernet link, 700-800 in GbE, etc.

Ethernet Switches

The switch is a key connecting device within IP surveillance networks. The primary function of a switch is to provide distribution for data within a network, with a typical role in a surveillance system of connecting cameras to recorders and recorders to viewing clients.

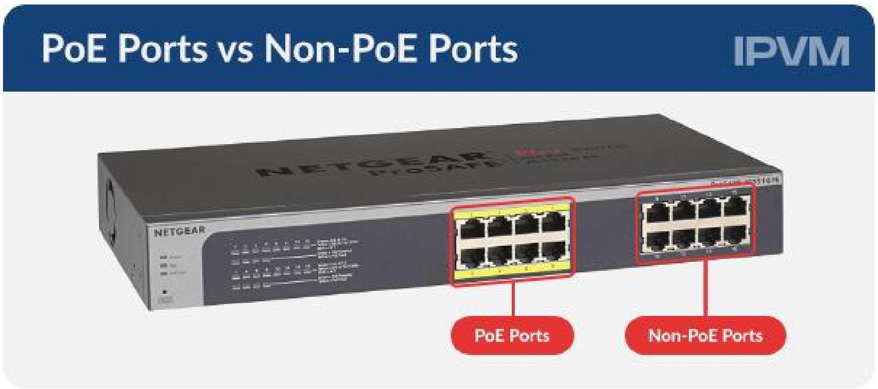
Both standalone and rackmount switches are common, usually ranging from 4 to 96 ports (or sometimes more) in a single box. At the high-end enterprise scale, multiple switches can be joined together into a single logical unit potentially comprised of thousands of ports.

Fast Ethernet models may be furnished with two or four GbE ports, which for surveillance applications is useful for connecting multiple switches together leading to a central recording server. Alternatively, a switch may come equipped with an SFP/+ port compatible for connecting the switch to fiber optic cables or another high bandwidth cabling format.

Our most recent statistics show that integrators still prefer Cisco switches over others, albeit by a smaller margin than in previous years.

PoE vs Non-PoE Switches

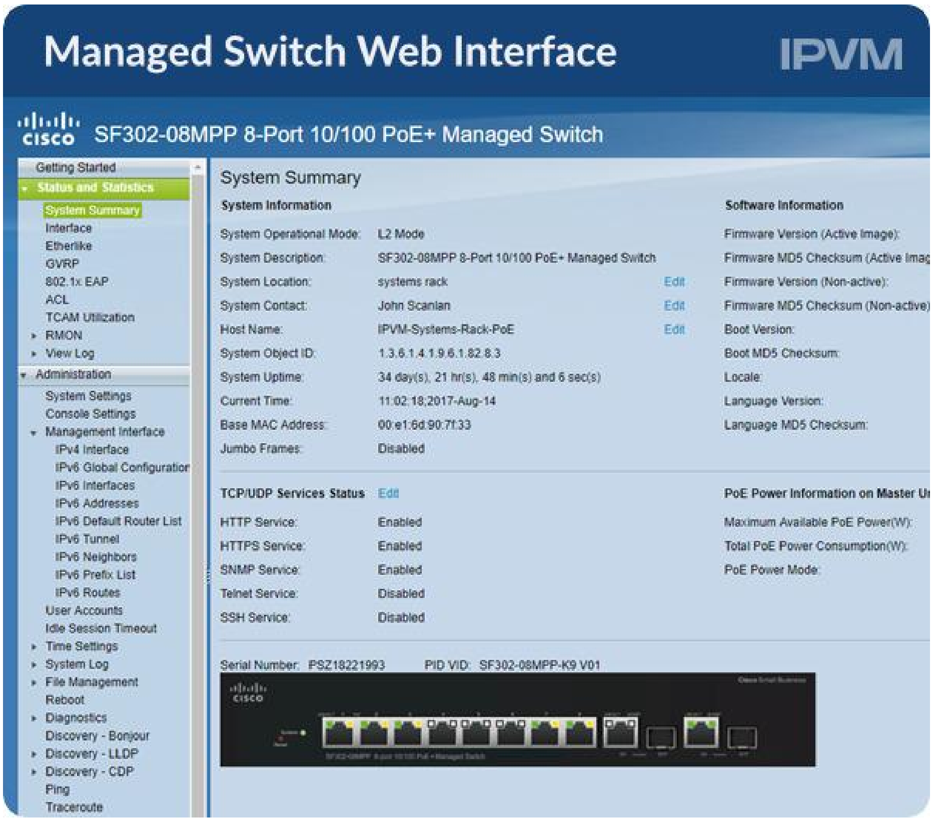
Statistically, most IP camera deployments use PoE switches. These are Ethernet switches that also power IP cameras connected to them. The key issues for PoE switches are how much total power they provide (many do not provide enough if all ports are powering IP cameras) and how many ports are PoE powered. Also, be sure to check how many ports on the switch are PoE capable, as it is commonly less than the total port count e.g. a 16 port PoE switch may only have 8 ports that provide PoE. For more, see our PoE Guide for IP Video Surveillance.



Managed Switches

Managed switches allow the user to connect, most commonly via web interface, to perform monitoring and setup tasks. Differing levels of management are available, normally referred to as "smart switches" versus "fully managed", though the features contained by each vary by manufacturer.

In surveillance, managed switches are more commonly used, as most PoE models (outside of very small, low-cost 4-5 port options) include some sort of management capability. Surveillance users may use the management interface to reboot cameras by cycling PoE power, set up network monitoring via SNMP, port mirroring for troubleshooting, segment surveillance traffic via VLANs, or configure multicast, all functions not found in unmanaged models. Below is the web interface of a Cisco managed switch.



System Summary

System Information

System Operational Mode: L2 Mode
System Description: SF302-08MPP 8-Port 10/100 PoE+ Managed Switch
System Location: systems rack
System Contact: John Scanlan
Host Name: IPVM-Systems-Rack-PoE
System Object ID: 1.3.6.1.4.1.9.6.1.82.8.3
System Uptime: 34 day(s), 21 hr(s), 48 min(s) and 6 sec(s)
Current Time: 11:02:18;2017-Aug-14
Base MAC Address: 00:e1:6d:90:7f:33
Jumbo Frames: Disabled

Software Information

Firmware Version (Active Image):
Firmware MD5 Checksum (Active Imag
Firmware Version (Non-active):
Firmware MD5 Checksum (Non-active)
Boot Version:
Boot MD5 Checksum:
Locale:
Language Version:
Language MD5 Checksum:

TCP/UDP Services Status

HTTP Service: Enabled
HTTPS Service: Enabled
SNMP Service: Enabled
Telnet Service: Disabled
SSH Service: Disabled

PoE Power Information on Master Ur

Maximum Available PoE Power(W):
Total PoE Power Consumption(W):
PoE Power Mode:

Serial Number: PSZ18221993 PID VID: SF302-08MPP-K9 V01

Unmanaged Switches

Unmanaged switches offer no configuration or monitoring capabilities, simply connecting devices on a single physical LAN. These switches are typically the lowest-cost models available, but should be used only in very small systems, typically 8 cameras and under, where monitoring and advanced configuration are not required.

Routers

While switches are used to connect devices together in a local network, routers are used to connect multiple networks. The router inspects network traffic, sending only packets addressed outside the local network through its WAN port to a modem (connected to the internet). Local traffic is kept internal.

While some routers are simply used to route network traffic, more commonly they include firewall features. This allows only specific traffic from specific devices through the router, based on rules set by users.

In surveillance, routers are most often used to connect the surveillance network to other networks, acting as a physical firewall. This allows the surveillance network to remain inaccessible except to those hosts which administrators choose.

Some routers additionally provide advanced features / services such as VPN.

Typically IP cameras are not connected directly to routers, they are connected to switches and then the switches are connected to the router.

Router/Switch 'Convergence'

Some routers may include switch ports, especially models intended for remote sites or consumer use. This eliminates the need for a separate switch in small networks. However, these ports are rarely PoE, so making direct camera connections requires a separate PoE midspan.

Also, some switches include routing functions. However, these devices are typically used in local area networks to more efficiently connect multiple VLANs than traditional routers, while routers are still used for higher security applications, such as connecting to the internet.

Media Converters - Fiber and Coax

Media converters adapt Ethernet from copper/UTP cables to fiber optics. Fiber optic cables support higher bandwidth, longer distances, and are immune to common types of interference which affect copper Ethernet cables.

In surveillance, fiber media converters are most commonly used to connect cameras more than 100m away from a switch to a standard network, such as pole-mounted cameras in parking lots. For more, see Daisy Chained Fiber Explained.

Another type of media converter common to surveillance is the Ethernet over Coax adapter. The specialized media converters allow users to reuse existing coaxial cables installed for analog camera systems to connect new IP cameras. We cover these in detail in our Ethernet Over Coax Shootout.

Ethernet Extenders

It is also possible to exceed distance limitations on typical UTP cabling far beyond the 100m max by using Ethernet extenders, which connect inline in long cable runs, regenerating the signal and passing PoE.

These devices essentially eliminate the need to install an IDF with its own switch at a given location to maintain standards compliant UTP cabling while reaching long distances.

Ethernet Network Distances

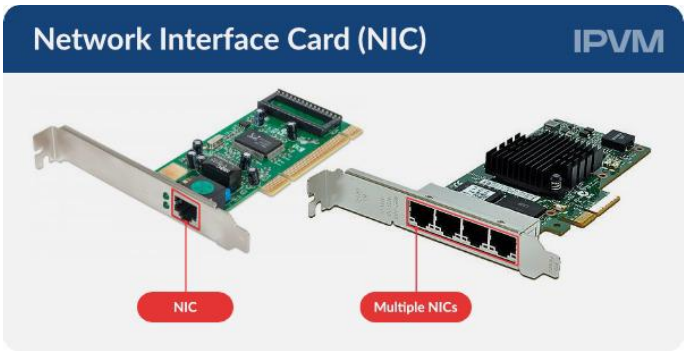
Another key element that remains constant, regardless of speed, is the distance between two devices. For Fast and Gigabit Ethernet over most types of UTP cable, the distance should not exceed 100m (330') per the guidelines set in IEEE802.3. Trying to stretch the distance longer leads to data reliability problems, usually causing video quality and communication issues between cameras, switches, and servers. For more see our long distance Ethernet test.

There are some manufacturers which claim longer Ethernet distances, which have functioned as advertised in our testing. However, these longer cable runs do not adhere to standards, which may be unacceptable to many users. Additionally, if standards-compliant equipment is used in the future, cable runs will need to be reconfigured, and switches and/or extenders added, etc.

Network Interface Cards

The Network Interface Card (NIC) performs the essential function of connecting a computer to a network. A "computer" might be a server or workstation, but could also describe an IP camera or NVR. In general, any device that accessible or managed on a network includes a NIC.

In modern use, NIC typically does not refer to a separate card installed onto a server's motherboard or camera's PCB. Instead, the NIC is often physically integrated with the computer it is matched with, and true dedicated Network Interface Cards are typically only found in servers:



Multiple Server NIC Usage

Usually, devices like cameras have a single network interface, but a server may have two or more. A common 'best practice' in terms of recorder performance and security is to physically segregate network connections to a dedicated NIC. A server might have two NICs, where one is connected to the network of cameras and the other is connected to a common LAN composed of workstations accessing video.

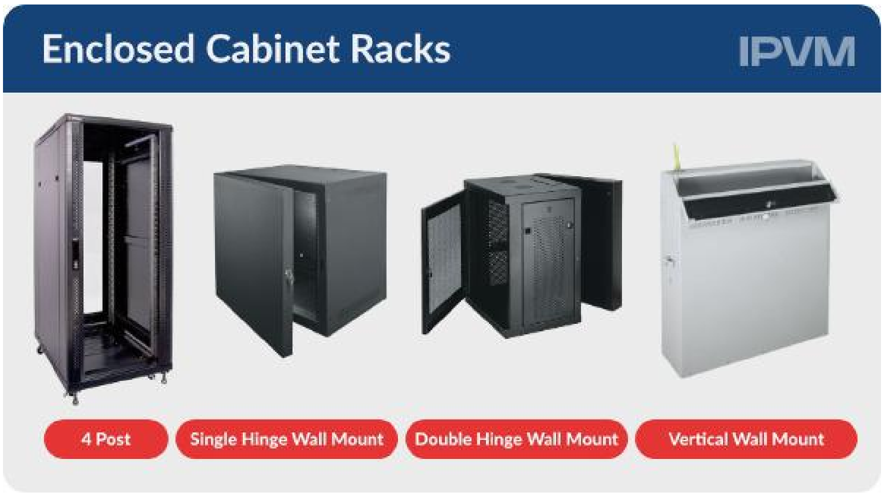
Every device network requires its own NIC. In mixed network environments including both wired and wireless networks, computers must have separate NICs for each. Each NIC has at least one IP address that declares its presence and location on a network.

Customer Premise Equipment

Those involved in surveillance networks may encounter the term "CPE", which stands for "customer premise equipment." CPE generally refers to equipment at the customer location, but not owned by customer, most often used to connect to another network, usually (but not always) the internet. Today, the most common types of CPE are cable and DSL modems and fiber optic interfaces (e.g. FiOS) used for most internet connections.

Racks and Cabinets

There are several types of enclosures for organizing as well as securing network equipment ranging from as single switch to full systems. These racks, cabinets, and mounts come in a variety of sizes and form factors and require special consideration for space, power, mounting, and other factors, covered in detail in our Network Racks For Surveillance Guide



Wireless

This guide is intended only to cover the basics of wired infrastructure. Wireless networking has its own considerations, design requirements, and hardware selections, covered in our Wireless For Video Surveillance Guide.

Network designers may need to consider space and connectivity in surveillance systems for some wireless hardware, such as controllers, but these are more often used in Wi-Fi systems, not surveillance.

Test your knowledge

Take this 10 question quiz now.

PoE

We provide comprehensive explanations of the elements in selecting and using Power Over Ethernet with IP cameras.

We cover:

- PoE vs Low Voltage
- When to Use PoE, When Not
- PSEs vs PDs
- PoE Classes
- 802.3af vs 802.3at vs 802.3bt
- Nonstandard PoE Implementations
- Passive PoE
- Spare Pairs
- Distance Limitations
- PoE Extenders
- Power Consumption vs Specification
- Calculating Power Budget
- PoE via Switch, MidSpan or NVR
- The Top 5 PoE Misunderstanding

PoE vs Low Voltage

All cameras need electrical power to operate.

'Power over Ethernet' (PoE) uses a single cable to connect a camera to both the data network and a power supply. In most cases, powering cameras before the advent of PoE meant using low voltage power using separate power supplies and dedicated power wiring. PoE eliminates the second cable / supply.

Using this single cable with power built into switches saves cost compared to low voltage power supplies, typically ~$10-30 per camera. See: PoE vs Low Voltage Power Supplies Cost Compared.

PoE Almost Always Used

PoE is supported and used, in practice, in almost all professional IP cameras and installations.

Exceptions To PoE Use

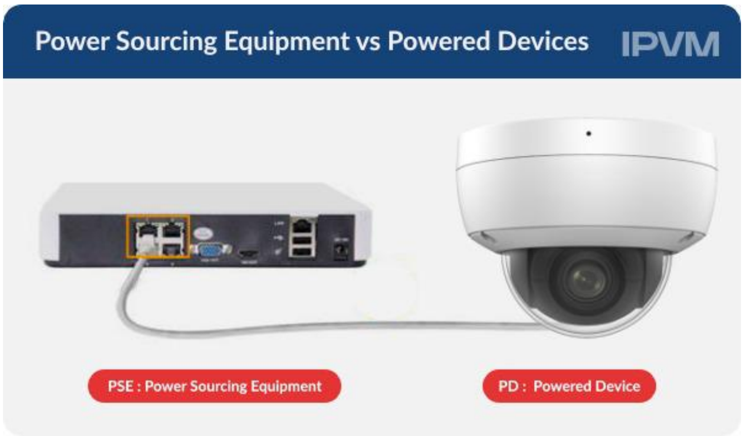
There are some exceptions where PoE is not used with IP cameras:

- *Fiber Ethernet*: In applications where cameras are connected via fiber, cameras are often powered via local low voltage power instead.
- *Solar power*: Sites powered via solar may prefer low voltage power to reduce conversions from 12/24VDC batteries to higher voltages required for PoE.

Additionally, many cameras today only support PoE creating logistical issues in those edge cases where low voltage power is required. For examples and details, see: Dealing with PoE Only Cameras.

PSEs vs. PDs

When looking at PoE specs, users may see the abbreviations PSE and PD used frequently. These are simply shorthand for Power Sourcing Equipment (switches, midspans, NVRs, etc.) and Powered Device (cameras, access points, controllers, etc.).


Power Sourcing Equipment vs Powered Devices
IPVM
PSE : Power Sourcing Equipment
PD : Powered Device

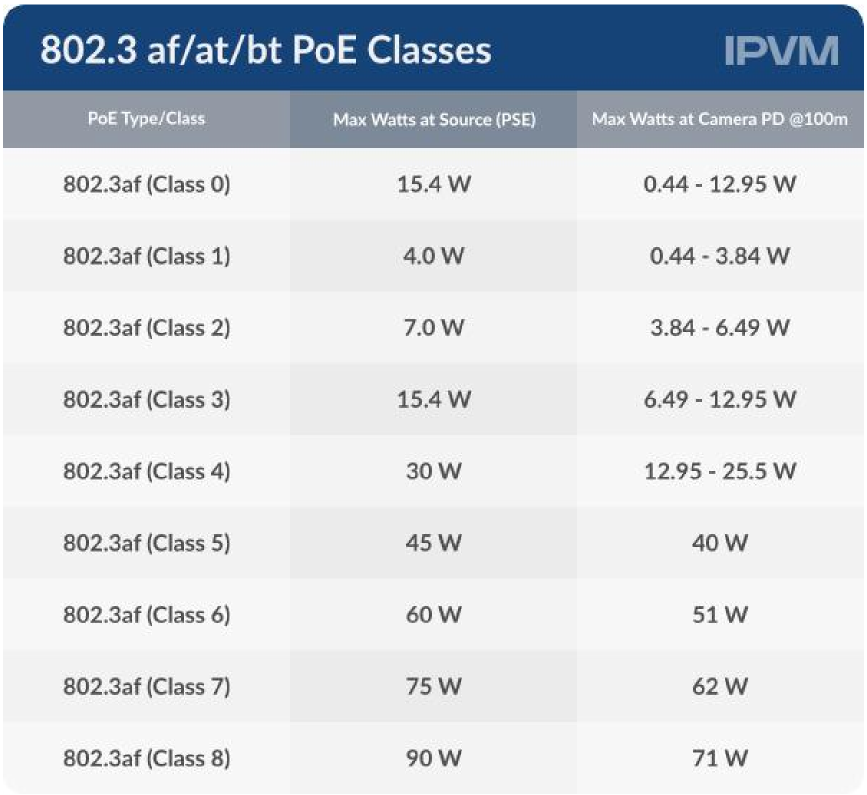
PoE Standards

PoE is defined by IEEE standards. These include:

- *802.3af*, which is the 'standard' PoE used by 90%+ of all IP cameras, supporting up to 15.4W
- *802.3at*, which is 'high' PoE used only by a small fraction of IP cameras that need more than 15.4W and up to 30W. 802.3at support is most commonly found / needed when dealing with PTZs or cameras with integrated heaters / blowers.
- *802.3bt*, recently ratified, with the potential for 100W PoE, that is beyond the needs of many IP cameras.

PoE Classes

PoE standards specify "classes" which segment / specify more precisely how much power the device consumes. The chart below summarizes the types and classes:



802.3 af/at/bt PoE Classes

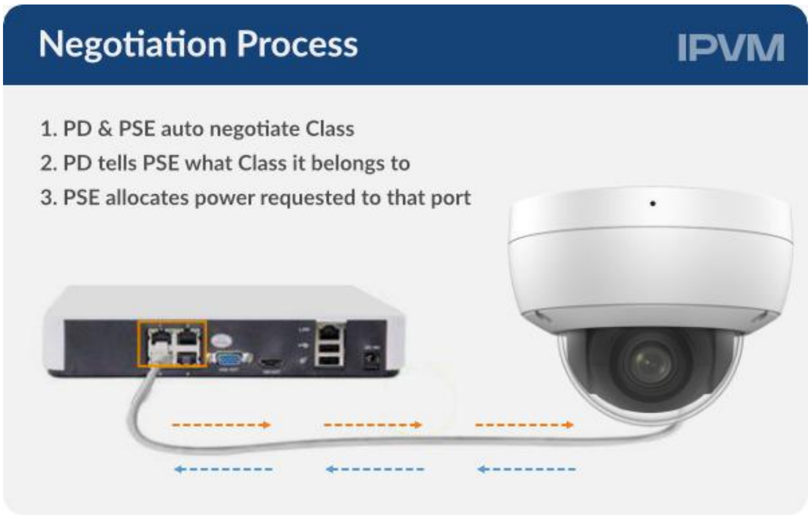
IPVM

PoE Type/Class	Max Watts at Source (PSE)	Max Watts at Camera PD @100m
802.3af (Class 0)	15.4 W	0.44 - 12.95 W
802.3af (Class 1)	4.0 W	0.44 - 3.84 W
802.3af (Class 2)	7.0 W	3.84 - 6.49 W
802.3af (Class 3)	15.4 W	6.49 - 12.95 W
802.3af (Class 4)	30 W	12.95 - 25.5 W
802.3af (Class 5)	45 W	40 W
802.3af (Class 6)	60 W	51 W
802.3af (Class 7)	75 W	62 W
802.3af (Class 8)	90 W	71 W

A formal PoE specification should include both a type and class, but that requirement is typically ignored. Most often, PoE is defined as '802.3af' only with no class modifier, meaning that anywhere between 0.44 to 15.4 W is available at the source. However, when a class is given, it limits further the minimum and maximum power available. For example, if a midspan is 802.3af Class 2 rated, it can only deliver a max of 7.0 watts.

PoE Negotiation

When connecting a powered device to a switch or other PSE, a negotiation process occurs, in which the device and switch determine the correct voltage and wattage and determine which class will be used. This process is quick, a matter of only a few seconds, and typically not observable by users.



Negotiation Process

1. PD & PSE auto negotiate Class
2. PD tells PSE what Class it belongs to
3. PSE allocates power requested to that port

Wattage Specs Are Not Classes

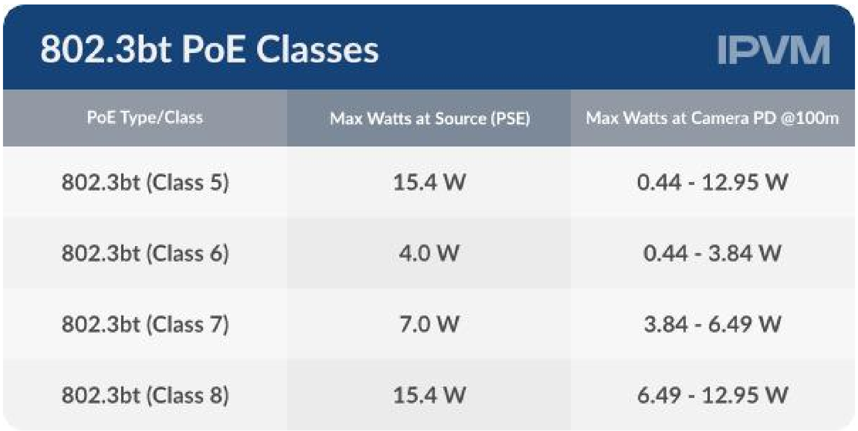
Note that while many cameras may list power requirements in their specs, this does not mean that a given camera will be seen as the class befitting that wattage by a PSE. For example, an IP camera with a specified power draw of 6W should fall into class 2, but is just as likely to be classified as 0. Users should not assume a given device will negotiate at a specific class unless it is listed on spec sheets, and even then, skepticism is healthy as many cameras are simply classified as 0 by PSE.

Class 0 Potential Issues

Regardless of actual consumption, many cameras are classified as Class 0 (max of 15.4W) by PSE. Because of this, switches may allocate more power than is required. So if 8 IP cameras requiring 7W each (56W total) are connected to a switch with a 60W power budget but classified as Class 0, cameras may not all power up or may cycle power. However, this is not always the case, with many switches ignoring class and simply allocating power based on actual draw.

Higher Power: 802.3bt Ratified In 2018

An even more substantial class of PoE (802.3bt) is was ratified in September of 2018. That standard provides a variant of PoE able to deliver 100 watts at the source by using all four pairs in a category cable, a point we cover in depth in the next section.



802.3bt PoE Classes

PoE Type/Class	Max Watts at Source (PSE)	Max Watts at Camera PD @100m
802.3bt (Class 5)	15.4 W	0.44 - 12.95 W
802.3bt (Class 6)	4.0 W	0.44 - 3.84 W
802.3bt (Class 7)	7.0 W	3.84 - 6.49 W
802.3bt (Class 8)	15.4 W	6.49 - 12.95 W

While the prospect of more than doubling 802.3at wattage is creating buzz, using it for surveillance gear may not be necessary, as most IP cameras consume less than 10W. The most likely markets for 802.3bt appear to be lighting systems, electrical motor controllers, and high powered industrial sensors. For more information please read our 802.3bt report.

Proprietary PoE

Not all devices claiming to be PoE use the 802.3at/af standards. Various manufacturers have released proprietary variants which offer higher wattages, such as Cisco's Universal PoE (60W) or Phihong's MegaPoE (95W).

In some cases, proprietary PoE implementations will work with standards-based devices, so an 802.3af camera may be connected to a UPoE switch, for example. In other variants, backwards compatibility is not guaranteed. Users should double check this compatibility before connecting equipment.

Passive PoE

In addition to the 802.3af/at/bt standards, some devices use so-called "passive" PoE, which injects 12 or 24 VDC onto spare cable pairs with no negotiation process used in standards based PoE. Power is supplied on these pairs whether the device "requests" it or not.

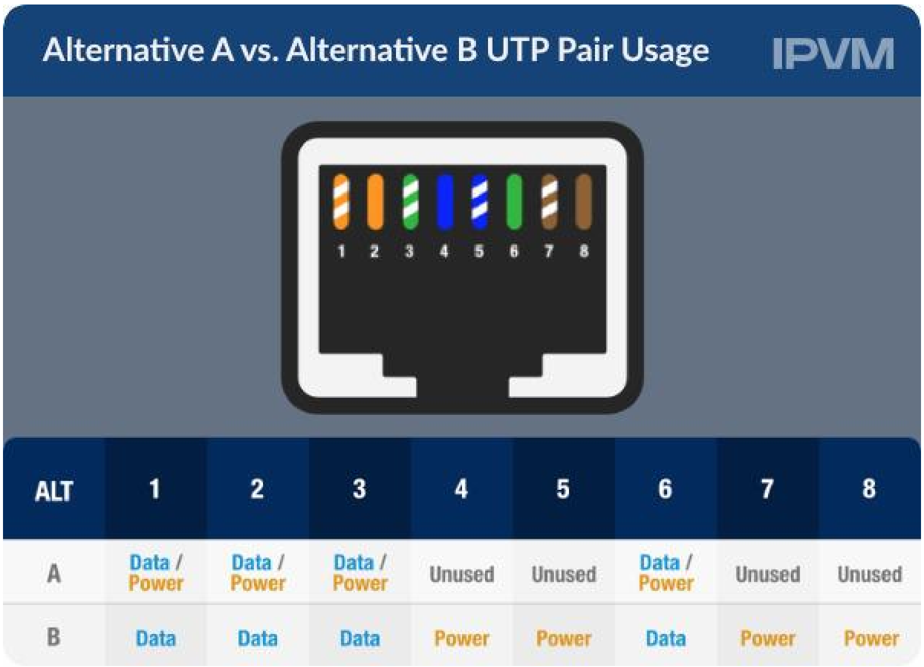
In some cases, powered devices may handle passive PoE without issue. However, those which are not specified to use may be damaged. Because of this, we do not recommend using passive PoE unless the device explicitly specifies it.

Passive PoE is most common in wireless equipment, such as Ubiquiti or Mikrotik, but not common in IP cameras.

Alternative A vs. Alternative B

PoE is supplied over different pins depending on the power source used, referred to as Alternatives A and B.

- Alternative A PoE injects power on the same pairs used for data (pins 1, 2, 3, and 6) with the remaining two pairs unused
- Alternative B injects power on unused pairs (pins 4, 5, 7, and 8)



Alternative A vs. Alternative B UTP Pair Usage

ALT	1	2	3	4	5	6	7	8
A	Data / Power	Data / Power	Data / Power	Unused	Unused	Data / Power	Unused	Unused
B	Data	Data	Data	Power	Power	Data	Power	Power

Most surveillance devices auto-sense which pairs are used to supply power. Many PoE devices are 'Alternate A or B agnostic' and will work without issue using either type of supply. However, some devices with only a minority of connectors (ie: Axis M12 connector) as Alternate Type specific. (The M12 is Type B PoE only.)

While the actual order of pins vary according to cabling standards (ie: TIA/EIA 568A or B), those standards affect the 2 data pairs, not the power pairs. Regardless of which wiring standard is used, if power sources and devices comply with the 802.3af/at spec, power connections will be made in the same way.

Distance Limitations

PoE is essentially limited to the same 100m distance limitation as of non-PoE Ethernet cabling. Data being carried by the cable will drop and degrade before the power drops below what the standard guarantees.

Beyond 100m, there are two typical options for extended length PoE: extenders and proprietary long length PoE.

PoE Extenders

For applications requiring more than 100m, PoE extenders are available. Typically, they are pairs of adapters for each camera, with power injected at the headend side. PoE extenders often provide 300m or even up to 600m total distance.

PoE extenders vary in price, but typically sell for $200-300 USD. For more, see Long IP Camera Run Options: Fiber, PoE Extenders and EoC examined.

Proprietary Extended PoE

Some manufacturers have released NVRs and switches which allow longer PoE distances, as much as 300-500m. This is typically achieved by using higher voltages (70-80VDC) to account for voltage drop at longer distances.

Note that these variants are not standardized and are specified to work only within a given manufacturer's product line (Uniview cameras with Uniview NVRs, for example). Using standard cameras on ports configured for extended PoE may cause damage to the camera.

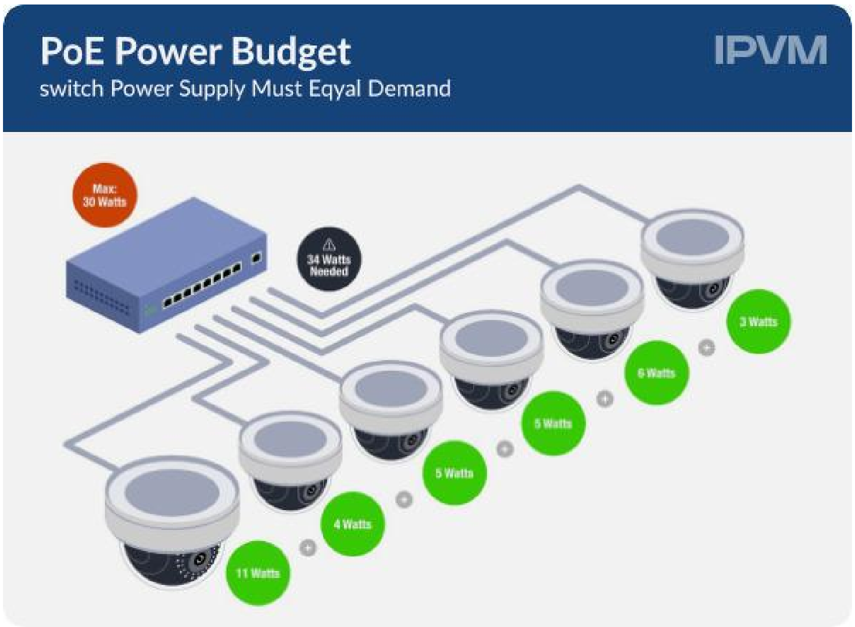
Typical PoE Consumption Vs Specification

Each IP camera manufacturer publishes specifications for power draw in addition to whether or not the camera supports PoE. This is important knowing how much total power you need as even if all cameras are 'regular' 802.3af PoE, power draw can range from as low as 2 watts to as high as 15. As a general rule of thumb, fixed IP cameras typically consume about 4 - 7 watts of power.

IP camera power specifications are typically higher than what is actually consumed by the camera, as verified in our IP Camera PoE Power Consumption Test.

Calculating Power Budget

Multiple IP cameras are typically powered by a single device. As such, one needs to check and add up the individual power requirements of cameras in one's system. For example, the six cameras below total 34W power draw, but the switch is able to supply only 30W total. Because of this, one camera will not power up or will cycle power repeatedly.



PoE via Switch or Midspan or NVR

PoE is typically provided in one of three ways:

- From a network switch that supports PoE
- Via a box installed in series with the cable called a midspan injector
- From an NVR with an embedded PoE switch

The network switch is, by far, the most common approach for providing PoE power. The midspan is used much less often though is preferred by some as it allows separating switch selection and support from midspan / PoE power. See: PoE: Switch vs. Midspan Usage

Switch Issues

With the use of PoE common in many areas, finding switches that offer PoE is not difficult.

However, care should be taken to confirm power is available on all switch ports. Especially in lower-end or consumer switch gear, it is common to enable PoE on one or half the available ports, but not them all:

Even 'professional' switches may only provide total power that is half of what is needed for full 802.3af support. For example, 12 port switches often support 90 total watts of PoE power, which is equivalent to 7.5 W per port. If you use IP cameras on all 12 ports, your use may require than 90 watts total.

In such cases, cameras can randomly go offline and be mistaken for a 'bad' camera when, in fact, is that the switch is turning off ports because it does not have sufficient power to support all cameras (see PoE Power Problems for more details). For a modest premium, some switches offer 'full' PoE power to all ports. In our 12 port switch example, this would be 180 watts (i.e., 15W x 12).

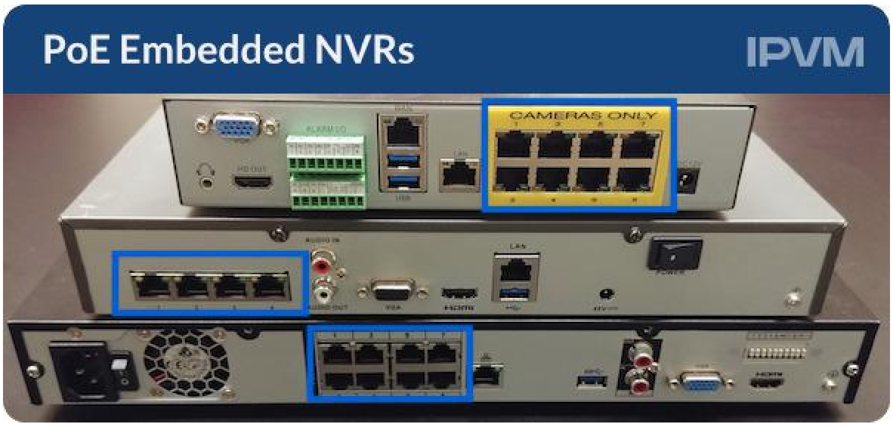
Midspans

The other option, midspan power injectors, are less commonly used but may be the right choice in applications where PoE cameras are desired but where a non-PoE network already exists, or where special PoE requirements can be satisfied more inexpensively than buying more expensive gear.For example, if 8 cameras are required, but only one is 802.3at, it may be more cost effective to buy a lower power 802.3af switch and a single 802.3at injector.

Typical Single Port PoE Midspan

PoE Embedded NVRs

Some NVRs have PoE switches built in, which has become a popular option for small systems. The main benefit of these units is simplicity, since buying / connecting to a separate PoE switch is eliminated.


PoE Embedded NVRs

Note that users should be especially careful when calculating power budget for use with PoE NVRs, as these units often support only lower power classes on all ports and may not support 802.3at.

Top 5 PoE Misunderstandings

In our guided IPVM IP Networking course, we include PoE as a core networking concept. Over the course of several sessions, certain questions are asked by students on a routine basis. Here they are:

1. Can I accidentally double PoE wattage by using midspans & switches together?
2. Does each port produce max rated wattage?
3. Can a cable plugged into a port, but not a camera electrocute me or be a safety hazard?
4. How far can PoE travel on cable?
5. Will cameras using power supplies be damaged by also plugging them into PoE ports?

In the sections below, we answer each question.

Question: "Can I accidentally double PoE wattage by using midspans & switches together?"

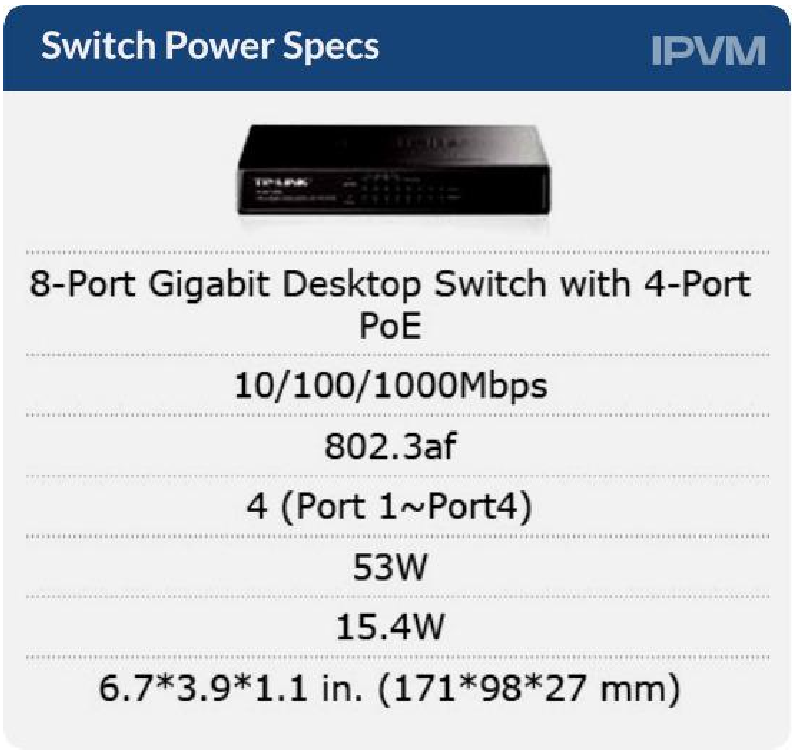
Answer: No. The process of devices using PoE generally involves a negotiation process where a device identifies and requests PoE power from a source like a switch or midspan injector. Because those source devices do not request power from potential sources, they do not themselves receive any PoE power. In this way, the 'only' PoE applied to the cable is done by the device nearest to the PoE powered camera or security device.

We tested this scenario in our PoE Midspan With Switch Tested report and describe the mechanics in full detail.

Question: "Does each port produce max rated wattage?

Answer: It is not guaranteed. While a port may be rated to deliver max wattage, (ie: 15.4W for 802.3af or 60W for 802.3at) the ability of the PSE to produce it depends on the total demand of PoE versus the maximum outputted power available. In many cases, demand outpaces supply, causing performance issues or brownout conditions for PoE devices.

For example, this consumer grade PoE switch (TPLink TL-SG1008P) has the following output specs:



Switch Power Specs

IPVM

8-Port Gigabit Desktop Switch with 4-Port PoE

10/100/1000Mbps

802.3af

4 (Port 1~Port4)

53W

15.4W

6.7*3.9*1.1 in. (171*98*27 mm)

The max PoE power available on the switch is 53W. With 4 PoE ports, this max power is divided between each, or: 53W / 4 ports = 13.25W per port. However, the max PoE power available per port is rated at 15.4W per 802.3af to 15.4 W * 4 = 61.6W. The difference between maximum port specifications and max output power available at the switch is a full 8.6W. This means if we had 4 cameras that required 15W each, the power budget would be overdrawn.

Question: "Can a cable plugged into a port, but not a camera electrocute me or be a safety hazard?"

Answer: No. Due to the initial negotiation process, PoE power is not actively issued unless a connected device requests it. This means that a cable connected to a PSE is not 'electrified' at all until plugged in to a PoE device and will not present a safety danger because of incidental contact.

Question: "How far can PoE travel on cable?"

Answer: The maximum 100m described by the ethernet IEE802.3 standard without using extenders or other means. By design, power will extend as far as any maximum length cable can be networked. In reality, this maximum length is much farther, per our IP Camera Long Distance Ethernet Test, where full PoE voltages were measured a full 1000' away from the source, beyond the point any data could travel on the same connected cable.

While PoE is rated for the max cable distance, any distance further than 100m does not meet ethernet standards, and additional lengths will not be supported and may void product warranties if used.

Question: "Will cameras using power supplies be damaged by also plugging them into PoE ports?"

Answer: Not likely, but beware. In most cases, cameras or other PoE devices will not request power even when available from a PSE if the device is already receiving power from a low-voltage power supply. However, especially with older PoE devices, instructions may warn against doing this at the risk of damaging the device.

In general, this is not an issue with newer cameras, but any disclaimers against this situation should be strictly heeded.

Test your knowledge

Take this 5 question quiz now

Cybersecurity

Keeping surveillance networks secure can be a daunting task, but there are several methods that can greatly reduce risk, especially when used in conjunction with each other.

We look at several security techniques, both physical and logical, used to secure surveillance networks, including:

- Network Hardening Guides
- Password Security
- LDAP / Active Directory Integration
- VLANs (Virtual LANs)
- 802.1X Authentication
- Disabling Switch Ports
- Disabling Network Ports
- Disabling Unused Services
- MAC Address Filtering
- Locking Plugs
- Physical Access Control
- Managing Network Security For Video Surveillance Systems

Cybersecurity Critical

More than ever, cybersecurity has become a key issue, with published vulnerabilities, hacks, and botnets on the rise.

In just the past 2 years, major vulnerabilities (and their effects) were reported in multiple manufacturers, including:

- Hikvision Backdoor Exploit: A hardcoded backdoor which allows attackers full control of Hikvision IP cameras.
- Dahua Hard-Coded Credentials Vulnerability: Hard-coded credentials were found in firmware for cameras and NVRs, allowing for rogue firmware uploads.
- Geovision 15 Backdoors and Vulnerabilities, including remote root access and clear text credentials
- TVT Backdoor, Hardcoded authentication to download remote system configuration - including login and password in clear text
- Axis Critical Security Vulnerability: A vulnerability allows attackers to remotely initiate a telnet connection, allowing the attacker to take over the device, reboot it, power it down, etc.
- Hacked Dahua Cameras Drive Massive Cyber Attack: As part of the Mirai botnet, hacked Dahua cameras (and others) took down major internet sites and even an entire country.
- See our Listings of Video Surveillance Cybersecurity Vulnerabilities and Exploits for more information on these and other issues, including new ones as they occur.

Because of the severity of these incidents and their increasing frequency, it is critical that users understand the basics of cyber security for surveillance systems, and how to protect against simple attacks at the very least.

Network Hardening Guides

In the IT industry at large, network hardening guides are common, outlining recommendations (as an example, see this Cisco hardening guide) to make the network more secure. Many/most of these recommendations apply to surveillance networks, as well, including controlling physical and login address, securing passwords, disabling ports, etc.

However, many recommendations may be above and beyond what many IP video integrators are capable of, or what is practical for a given system. Complex authentication schemes such as 802.1x, LDAP integration, SNMP monitoring, etc., are simply not worth the time/cost to implement for many systems, given the limited risk.

Surveillance Hardening Guides Increasingly Common

Unlike IT, surveillance specific hardening guides have historically been rare. However, this number has doubled in the past 2 years

- Axis cyber hardening guide
- Bosch IP Video and Data Security Guidebook
- Dahua Product Security Hardening Guide
- EagleEye Networks Security Camera Best Practices
- Genetec cyber hardening guide (requires partner login)
- Hanwha Network Hardening Guide
- Hikvision Network Security Hardening Guide
- Milestone cyber hardening guide
- OnSSI Hardening Guide
- Salient Video Surveillance System Hardening Guide
- Vivotek Security Hardening Guide

The exact recommendations in each of these guides vary, but most are divided into basic and advanced levels, depending on the criticality of the installation.

The Axis guide, for instance, varies from demo only (not production use) to highly secure enterprise networks, and include basic best practices, such as strong passwords, updating firmware, and disabling anonymous access, through more complex practices, such as 802.1x authentication, SNMP monitoring, and syslog servers.

While these guides are manufacturer-specific, providing instructions pertinent to the camera or VMS, many recommendations are useful across all manufacturers, and fall in line with IT industry best practices, and the practices discussed below.

Strong Passwords

Strong passwords are the most basic security measure, but unfortunately, ignored by many users. Many surveillance systems are deployed in the field with default passwords on all equipment, including cameras, switches, recorders, and more (see our IP Cameras Default Passwords List). Doing so may make it easier for techs to access cameras but also make it simple for anyone to log into one's cameras (see: Search Engine For Hacking IP Cameras).

At the very least, all surveillance network devices, including cameras, clients, and servers, should be changed from the defaults with strong passwords, documented in a secure location. This prevents access to the network using simple password guessing, requiring a more skilled attacker and more complex methods.

Some manufacturers require changing the default password when connecting for the first time (see a comparison of how Axis, Dahua and Samsung set passwords). Indeed, an upcoming ONVIF Profile (Q) would make changing default passwords mandatory, though how well that is adopted remains to be seen.

LDAP/AD Integration

Using LDAP/Active Directory (AD) integration, VMS permissions are assigned to network users managed by a central server (also called single sign-on). Since these user accounts often implement password strength and expiration rules, this integration may improve security over local VMS accounts which do not have these restrictions. This reduces administration overhead, since individual accounts do not to be created and maintained.

Typically, LDAP use is restricted to larger, enterprise systems, since many small installations do not have an LDAP server implemented. Some small or midsize systems which are installed in larger entities, especially education and corporate facilities, may use LDAP as these organizations are likely to use it for their network access control.

LDAP / AD could theoretically be used for IP cameras, but, in practice is not. ActiveDirectory, as a Microsoft offering, is not supported by almost any IP camera, which typically run on Linux. One Windows IP camera claimed to do so, but it has not gained any meaningful market share.

Firewalls/Remote Access

To prevent unauthorized remote access, many surveillance systems are not connected to the internet at all, instead on a totally separate LAN. This reduces risk, but may make service more difficult, as updates to surveillance software and firmware, usually simply downloaded, must be loaded from USB or other means.

Those systems which are connected are typically behind a firewall, which limits inbound/outbound traffic to only specific IP addresses and ports which have been authorized. Other traffic is rejected. Properly implemented, this may prevent the vast majority of attacks. Like cameras and other surveillance equipment it is important to keep routers firmware up to date. There have been two major security vulnerabilities related to insecure routers. The first is a vulnerability in Cisco firmware, and the other is the Russian government targeting infrastructure in part by attacking insecure SOHO / SMB routers.

Remote Access Risks

For devices which require remote access, VMSes and cameras may require one or more ports to be open. However, each open port presents a possible opportunity for an attacker. Exactly how many and which varies by the VMS. Users should refer to manufacturer documentation for which ports must be open if remote access is required (for maintenance or remote viewing), and we list some examples in our Network Ports for IP Video Surveillance Tutorial.

P2P/Cloud Access

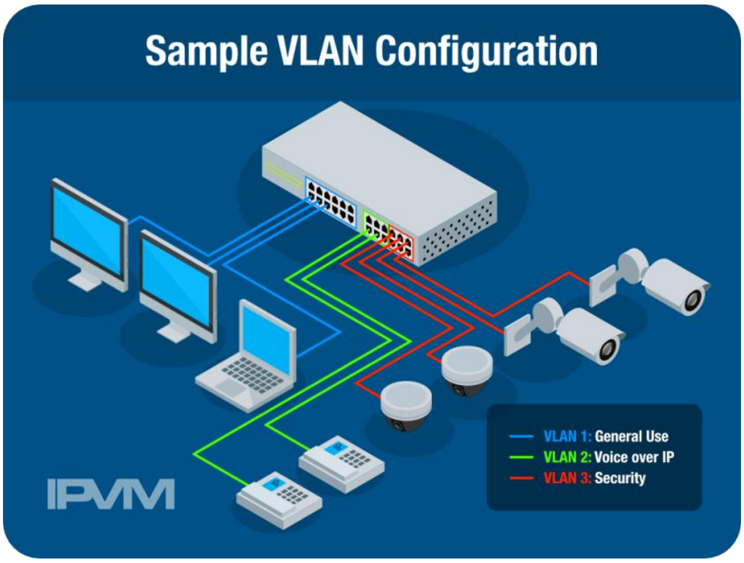
Alternatively, some manufacturers allow for "phone home" remote access, which sets up a secure tunnel via an outbound connection without requiring open ports, reducing risks. Many cameras and recorders use cloud connections for remote access, such as Hikvision EZVIZ, Eagle Eye Cloud VMS, and Genetec Cloud. Additionally, many remote desktop services use similar technology, such as LogMeIn, TeamViewer, SplashTop, etc.

We discuss these methods in our Remote Network Access for Video Surveillance tutorial.

VLANs

Virtual LANs (shortened to VLANs) improve security by segmenting traffic into multiple virtual networks. So while other services, such as IP based surveillance equipment or general office LAN traffic, may exist on the same physical switch, for practical purposes the networks are invisible to each other, and unreachable.

For example, in the image below, the surveillance equipment on VLAN 3 may not be reached by the office PC on VLAN 1, nor could a user on the camera (VLAN 3)"see" traffic on the VoIP VLAN (VLAN 2).



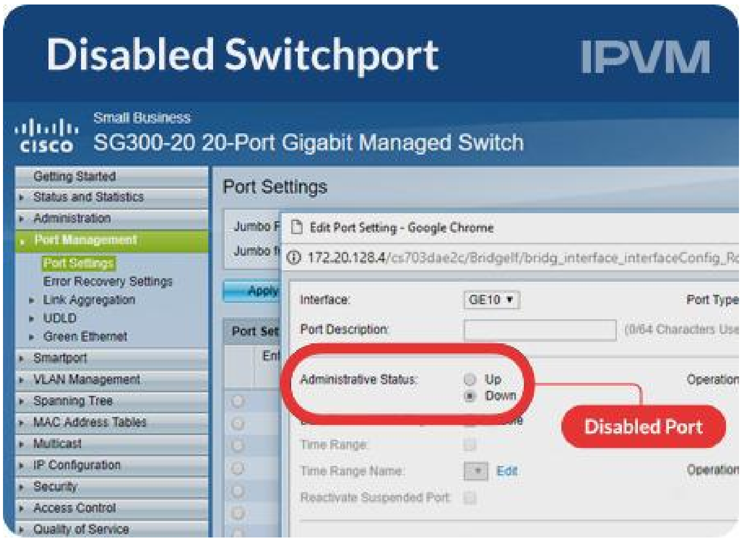
VLANs are most commonly set up using 802.1Q tagging, which adds a header to each frame containing VLAN information. This header is interpreted by the switch and traffic forwarded only to other devices on the same VLAN.

Note that while traffic may not be intercepted across VLANs, bandwidth constraints still exist. Numerous large video streams may negatively impact VOIP and office application performance, while large file transfers may affect the surveillance network. Because of this, VLANs are also most often deployed in conjunction with [Quality of Service (QoS)](), which prioritizes network traffic, sending video packets ahead of file transfers, for example, so video quality is not impacted.

See our [VLANs for Surveillance]() guide for further information.

Disabling Unused Switch Ports

Another easy but typically overlooked method of keeping unauthorized devices from accessing a switch is to disable all unused ports. This step mitigates the risk of someone trying to access a security subnet by plugging a patch cable into a switch or unused network jack. The option to disable specific ports is a common option in managed switches, both low cost and enterprise:



Disabled Switchport

Edit Port Setting - Google Chrome

172.20.128.4/cs703dae2c/Bridgelf/bridg_interface_interfaceConfig_Ro

Interface: GE10 ▾

Port Description:

Administrative Status: ○ Up ● Down

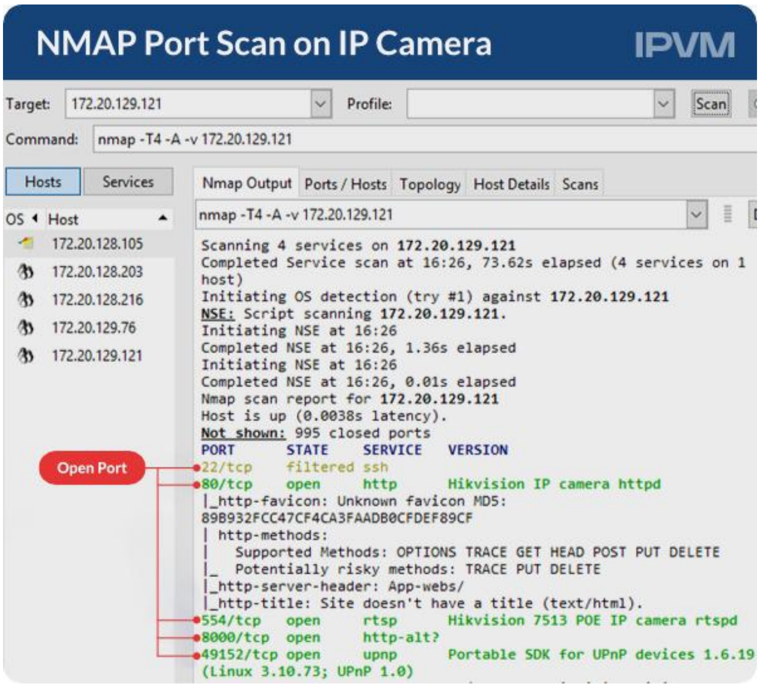
Disabled Port

While effective at narrowing the number of potential access points, this step does not necessarily prevent unauthorized access to a network, as someone could potentially unplug a device (camera, workstation, printer) from a previously authorized port or jack and access its port, unless measures such as MAC filtering or 802.1X are in place.

Disabling Unused Network Ports

Many cameras ship with unneeded network ports turned on, such as Telnet, SSH, FTP, etc., as we found in our NMAPing IP Cameras Test. These ports are favorite targets of hackers (as illustrated by bitcoin miners and buffer vulnerabilities found in Hikvision Cameras).

A quick 30 second scan of a popular IP camera reveals multiple open ports other than those expected for web access and video streaming (80/554):



NMAP Port Scan on IP Camera

Target: 172.20.129.121

Profile:

Command: nmap -T4 -A -v 172.20.129.121

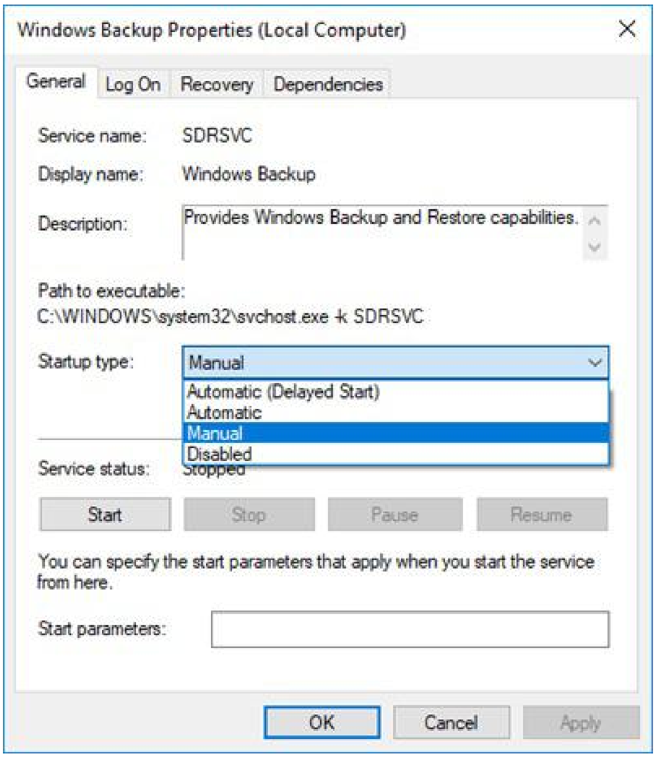
```
nmap -T4 -A -v 172.20.129.121
Scanning 4 services on 172.20.129.121
Completed Service scan at 16:26, 73.62s elapsed (4 services on 1
host)
Initiating OS detection (try #1) against 172.20.129.121
NSE: Script scanning 172.20.129.121.
Initiating NSE at 16:26
Completed NSE at 16:26, 1.36s elapsed
Initiating NSE at 16:26
Completed NSE at 16:26, 0.01s elapsed
Nmap scan report for 172.20.129.121
Host is up (0.0038s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE   VERSION
22/tcp    filtered ssh
80/tcp    open     http      Hikvision IP camera httpd
|_http-favicon: Unknown favicon MD5:
89B932FCC47CF4CA3FAADB0CFDEF89CF
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST PUT DELETE
|_  Potentially risky methods: TRACE PUT DELETE
|_http-server-header: App-webs/
|_http-title: Site doesn't have a title (text/html).
554/tcp   open     rtsp      Hikvision 7513 POE IP camera rtspd
8000/tcp  open     http-alt?
49152/tcp open     upnp      Portable SDK for UPnP devices 1.6.19
(Linux 3.10.73; UPnP 1.0)
```

These ports should be disabled wherever possible to prevent potential attacks.

Disabling Unused Services

Unnecessary services on viewing workstations and servers should be turned off. These may include manufacturer-specific update utilities, various Microsoft update services, web services, etc. These unneeded services may act as a backdoor for hackers or viruses, consume additional processor and memory, and increase startup time.

These services should be disabled or set to operate only when manually started, as seen here in Windows:



Windows Backup Properties (Local Computer)

Service name: SDRSVC

Display name: Windows Backup

Description: Provides Windows Backup and Restore capabilities.

Path to executable:
C:\WINDOWS\system32\svchost.exe -k SDRSVC

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OS and Firmware Updates

OS and firmware updates are a matter of some debate, with some users installing every available Windows Update, for example, while others insist that these updates may break VMS software or camera integrations.

However, these updates (especially Windows Update) often include patches to newly discovered security vulnerabilities, such as the Heartbleed SSL vulnerability, which affected millions of computers worldwide. Patches for these significant issues should be installed.

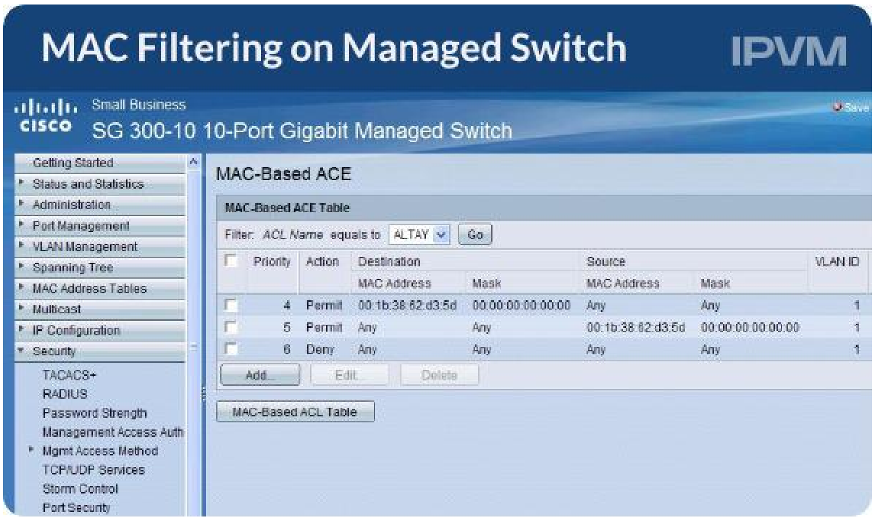
Other, more routine, updates may be optional. Users especially concerned about compatibility issues should contact their camera/recorder/VMS manufacturers to see their recommendations for applying updates or not.

MAC Address Filtering

MAC address filtering allows only a specific list of devices to connect to the switch. Other devices plugged into the switch are ignored, even if the port previously was used by a valid device. MAC filtering is possible only using managed switches.

In surveillance networks, MAC filtering is typically easy to administer. Once all cameras, clients, and servers are connected, it is enabled, and connected devices' MACs added to the whitelist. Since these devices in a surveillance network are rarely changed out, little extra maintenance is required. In other networks where devices may frequently be added or removed, administrators may find filtering more cumbersome to administer.

This image shows MAC filtering options in a typical managed switch interface:



MAC Filtering on Managed Switch

MAC-Based ACE

MAC-Based ACE Table

Filter: *ACL Name* equals to ALTAY Go

□	Priority	Action	Destination		Source		VLAN ID
			MAC Address	Mask	MAC Address	Mask	
□	4	Permit	00:1b:38:62:d3:5d	00:00:00:00:00:00	Any	Any	1
□	5	Permit	Any	Any	00:1b:38:62:d3:5d	00:00:00:00:00:00	1
□	6	Deny	Any	Any	Any	Any	1

See our Network Addressing for Video Surveillance Guide for more discussion and a basic overview of MAC addresses.

802.1X

802.1X requires devices trying to connect to the network to have proper credentials to be allowed on. This blocks random devices or attackers from just jumping on a network.

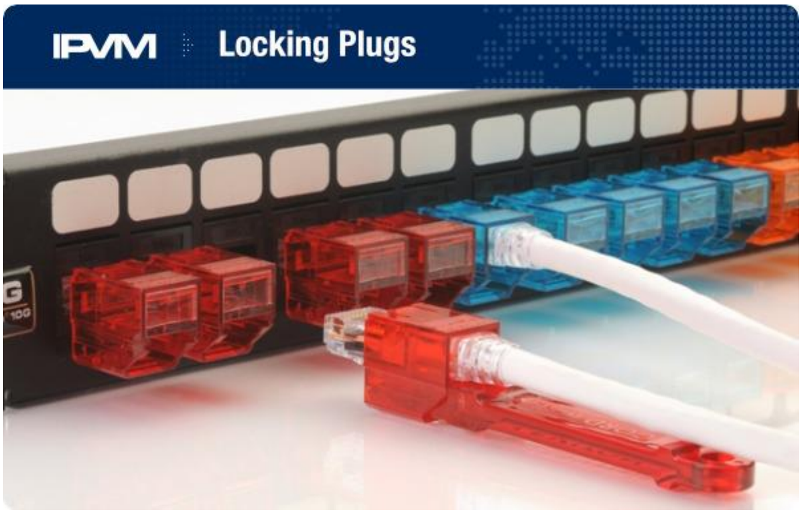
Using 802.1X, a "supplicant" (client such a camera, PC, etc.) attempts to connect to network via a switch or WAP (called the "authenticator"). The authenticator then checks the credentials of the supplicant with a server, call the authentication server (typically using a protocol called RADIUS, and grants or denies access accordingly.

While 802.1X provides strong security, setting up a network to support it can be cumbersome and involved. Not only must connected devices (cameras, WAPs, client PCs, NVRs, etc.) support 802.1X integration, all switches must, as well. Each of these devices must be individually configured for 802.1X, adding additional configuration time to the install.

Because of these factors, which increase cost and administration overhead, 802.1X is rarely used in all but the most complex enterprise surveillance networks, with users opting for simpler security measures instead.

Locking Plugs

Another layer of security that physically prevents connection or tampering with network cabling by unauthorized devices are port plugs and cable locks. These devices mechanically lock a cable into a switch, patch panel, or wall jack, or fill unused switch ports, and may only be removed with a proprietary tool.



While these types of locks are effective at stopping casual tampering, they are not unbeatable or indestructible, and a determined intruder may simply be able to force them out or pry them loose given enough time. As such, locking plugs should be considered part of a good network security program, but not the only element.

For a deeper look, read our Locking Down Network Connections update.

Door Locks and Physical Access

Finally, best practices call for controlling access to the most vulnerable areas of a network, the rooms, closets, or racks where surveillance servers and switches are typically mounted. By reducing the potential availability of these areas, many risks from determined or even inadvertent threats can be avoided. If doors cannot be secured, individual rack cages or switch enclosures should be. Most modern IT cabinetry includes security equipment as standard options:

As a result, many facilities employ electronic access control on server or network equipment rooms. However, even non-exotic mechanical keys and locks can do a great job of protecting sensitive areas when properly managed.

Managing Cybersecurity For Video Surveillance Systems

While all the steps below may improve security on their own, they are most effective when documented as part of a written (and enforced) security policy.

In surveillance, this policy is up to the individual install, but general,ly it comes from one of two places:

- *End user*: When the surveillance network is part of a larger corporate/enterprise LAN (whether sharing switches or dedicated), end users most likely control the security policy for all network devices, and may force these requirements upon integrators (for better or worse).
- *Integrator*: If an end user does not have a security policy in place, the installing integrator may choose to create one as part of their documentation, requiring it to be followed in order for the warranty to be enforced and limit liability in case of a breach.

Test your knowledge

Take this 12 question quiz now.

Wireless Networking

Wireless networking is a niche in video surveillance applications, but it can be a difficult one to understand with proper wireless design, equipment selection, interference, and other factors impacting it usage.

We break down the key elements of wireless networking for video surveillance:

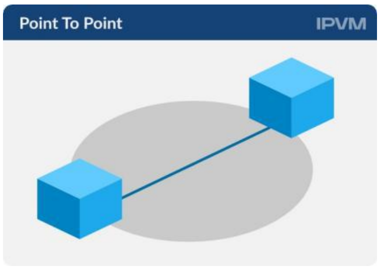
- Topology: PTP vs PtMP vs Mesh
- Antennas: Internal vs External
- Antennas: Omnidirectional vs Directional
- Antennas and Gain
- Free Space Path Loss
- Frequencies Including Licensed and Unlicensed Ranges
- MIMO Radios
- Bandwidth Planning
- Transmission Range
- Wireless Products Specializing in Surveillance
- Maintenance
- Power Requirements

Topology

There are three basic wireless network topologies in use in surveillance, with varying uses depending on where and how cameras are deployed:

- Point-to point
- Point-to-Multipoint
- Mesh

Point-to-Point



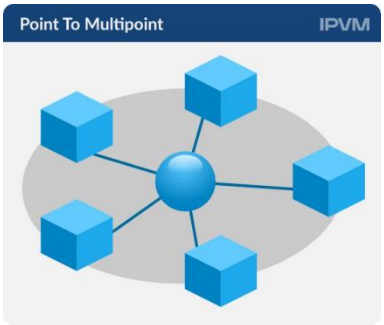
First, and most common are point-to-point (PtP) wireless links. In PtP networks, a single radio at the device location is connected to a single radio connected to the surveillance network. PtP links are used in two common applications:

- *Connecting cameras*: Most commonly, PtP radios are used to connect cameras from a single location (such as a parking lot pole, for example) to a surveillance system.
- *Wireless backhaul*: Point to point is also used in backhaul applications, connecting two buildings together or connecting a multipoint base station to another point in the network.

Directional antennas are most often used in PtP applications, with multi-mile ranges possible. Many different frequency options are available, from 900 MHz, to 2.4 and 5.8 GHz, and higher.

Point-to-Multipoint

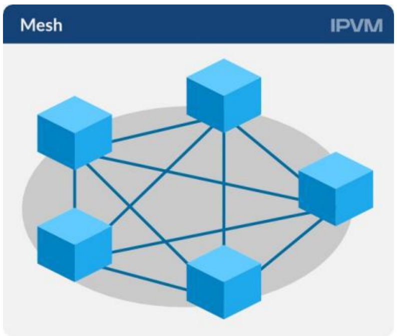
In point-to-multipoint (PtMP) wireless links, a single radio acts as base station, connected to the central network, with multiple radios transmitting to it. The radios used in PtMP setups may be the same as PtP in many cases, though some manufacturers use special radios for the base station to handle higher data rates possible when connecting numerous client radios.



PtMP is used in applications where multiple cameras must be dispersed around the area, without dedicated wired connectivity, with each camera sending video to the base station These systems range in size from a handful of cameras in a parking lot to city-wide surveillance systems, where clusters of cameras are connected via PtMP before being backhauled through other means.

PtMP base stations typically use omnidirectional or wide angle directional antennas (such as sectors), depending on whether cameras are located in all directions or in one general direction. PtMP client radios most often use narrower directional antennas.

Mesh



In a mesh network, each wireless node connects to two or more other radios, providing more than one path for network traffic. If one link fails, data is rerouted to another path, reducing the chance of a total outage. However, if failover is desired, the mesh must be carefully designed to handle failed links, or traffic from one may quickly overload another.

Historically, mesh radios were typically more expensive than PtP or PtMP models, and more time-consuming to configure. Because of this added expense, it was most often seen in city surveillance, one of the few applications with both the budget and need for these failover capabilities.

However, mesh node pricing has dropped and speeds (<$100 USD in some cases) have increased significantly (over 1 Gb/s), making mesh available in more applications. Additionally, mesh has become available to residential customers with kits from Google, Netgear, and others to expand Wi-Fi coverage throughout homes/businesses.

Mesh radios may use any type of antenna, depending on the distance to other nodes, and how many it is connecting to.

Internal Antennas for IP Cameras

Having wireless built into an IP camera is statistically rare and the cameras that do have integrated wireless, typically have short ranges and are marketed for consumer use, not professional.

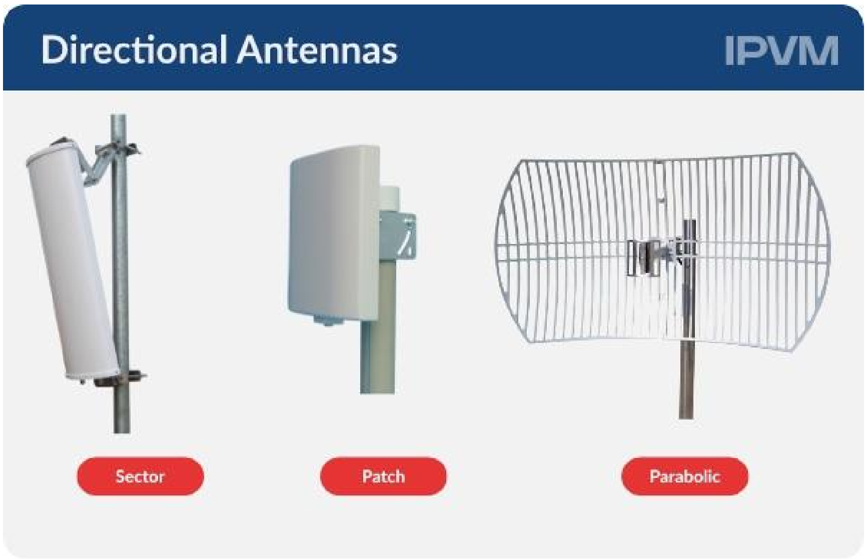
As such, most professional video surveillance applications use standard wired IP cameras, without integrated wireless, connected to an external wireless radio using proper antennas.

Omnidirectional Antennas

Omnidirectional antennas radiate the signal in all directions. Most users are familiar with this type of antenna as it is typically included with consumer wireless routers, the black "rubber ducky" style as well as the "blade" seen below. Outdoor models function the same way, but may be much larger (3-5' long), depending on desired gain.

Directional Antennas

Directional antennas are available in numerous styles with varying beamwidths. Some provide tight coverage, 15 degrees horizontal or less, while other may be wide, over 100 degrees. Note that antenna type (sector, patch, parabolic, etc.) does not necessarily reflect beamwidth, and a wide variety of options are available in each form factor.



Performance Tradeoffs

Selecting the proper antenna depends on many factors, but essentially comes down to these tradeoffs:

- Omnidirectional antennas are easiest to set up, requiring little or no alignment, but offer the shortest range. They should be used only when required to connect multiple cameras to a base station, for example.
- Directional antennas such as patch and sector provide better range performance due to their narrower beam pattern. They are most commonly used both as external antennas and those built into all-in-one radios. They may often be aimed by sight instead of requiring more complex signal strength metering and aiming, and are forgiving of small changes due to wind, sway, and vibration.
- Highly directional antenna such as parabolic provide the strongest signal, but are difficult to aim due to their narrow beamwidth, often requiring experienced technicians to install. These antennas are most often aimed using lasers, signal strength meters, and other more complex means, and are more susceptible to performance issues due to sway or vibration than other types.

Antenna Impact On Gain

Gain is important because the higher the gain, everything else being equal, the further the signal can transmit and more likely it can deal with obstructions. Omnidirectional antennas are often as low as 3dB while directional antennas can be 24dB or higher.

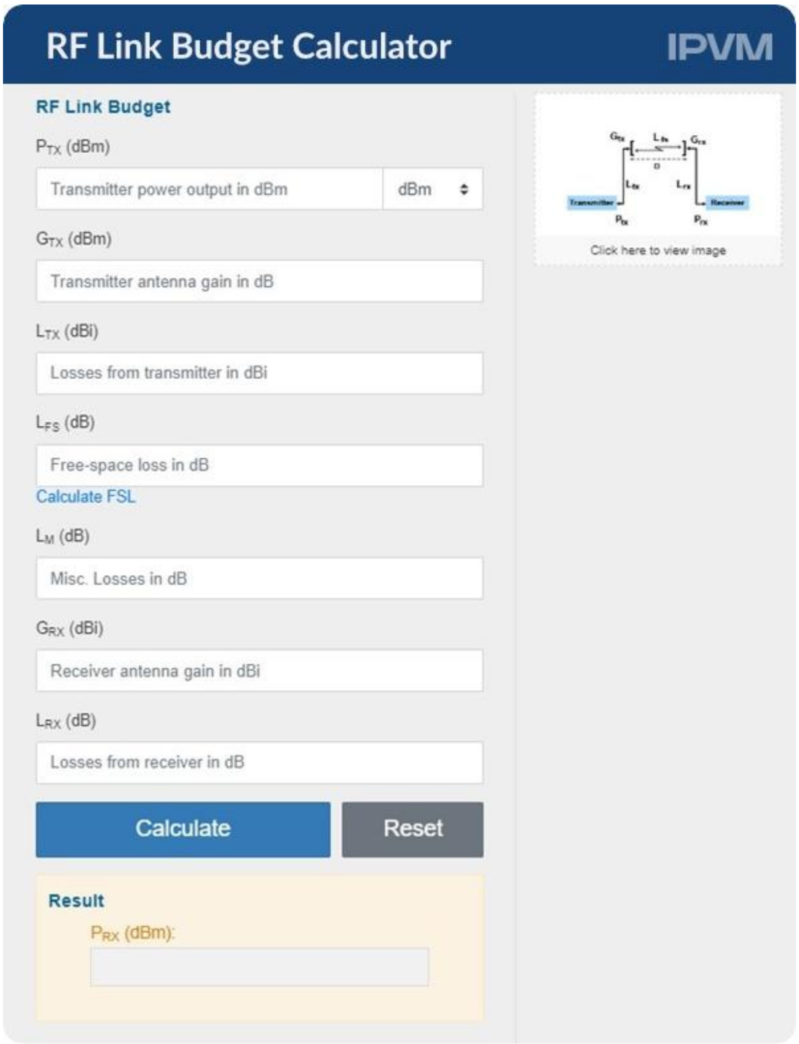
Free Space Path Loss

In this section, we introduce the basics of figuring out how far a signal can transmit, aka calculating free space path loss, for more, see: Training: RF for Wireless Surveillance.

The factors that drive how far one can transmit include:

- The frequency being used: higher the frequency, the shorter one can go (e.g., 5.8Ghz, everything else equal, has shorter range than 2.4Ghz).
- The gain of the antennas being used: the higher the gain (e.g., 24dB instead of 12dB), the farther one can go.
- The sensitivity level the receiver requires. The higher the level, the easier it is to meet but typically less bandwidth is available (e.g., -96dBm vs -74dBm for higher bandwidth levels).
- The transmission power of the radio. Most surveillance wireless systems use licensed frequencies which cap how much power can be put out, constraining how far the signal can go (unlike, e.g., a TV station which is comparatively 'blasting' out transmissions at much lower frequencies).

Because of the complex calculations required in FSPL, RF link budget calculators are most often used, with user inputting distance, frequency, antenna and cable information, and receiver sensitivity. The output of one of these calculators for a sample 5.8 GHz link is shown below.



RF Link Budget

P_{TX} (dBm)

Transmitter power output in dBm | dBm

G_{TX} (dBm)

Transmitter antenna gain in dB

L_{TX} (dBi)

Losses from transmitter in dBi

L_{FS} (dB)

Free-space loss in dB

Calculate FSL

L_{M} (dB)

Misc. Losses in dB

G_{RX} (dBi)

Receiver antenna gain in dBi

L_{RX} (dB)

Losses from receiver in dB

Calculate | Reset

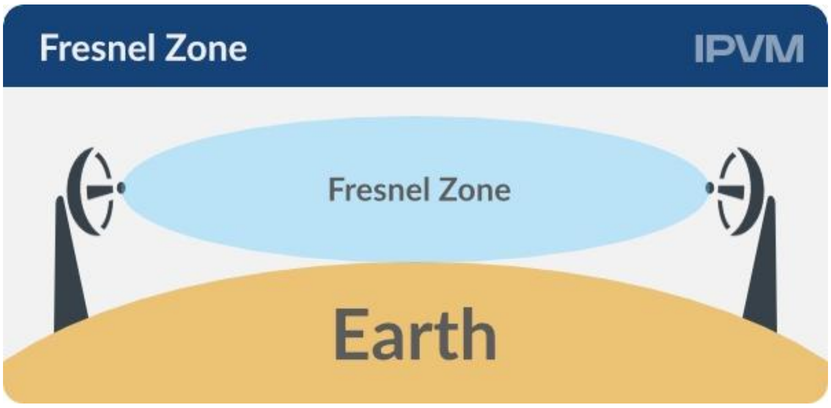
Result

P_{RX} (dBm):

Fresnel Zone

Although it's easy to think of wireless signal as a line or a cone, it is actually an elliptical region between the transmitter and receiver, called the Fresnel Zone. Simply put, the larger the distance between the radios, the larger the diameter of the fresnel zone.

Because of this, the curvature of the earth may become an issue at very long ranges (over several miles) as the ground begins to enter the fresnel zone, requiring radios to be mounted higher to compensate. Additionally, at shorter ranges, users should beware of other obstructions, such as trees, passing trucks, or buildings entering the fresnel zone, as they may also cause absorption/reflection issues.



Calculators are commonly used to calculate the size of the fresnel zone and corresponding mounting height, similar to link budget calculators. Manufacturers may offer their own calculator, but many generic calculators are readily available online.

Obstructions / Line Of Sight

Though some frequencies may penetrate obstructions better than others, wireless links should ideally have clear line of sight (LOS) between radios for best performance. Obstructions impact performance in three key ways:

- Absorption
- Reflection
- Multipath Propagation

When RF hits an obstruction, some of the signal is absorbed and/or reflected, reducing the level of signal reaching the receiving end. How this impacts performance depends on the material. For example, drywall and wood studs (common home and office construction materials) absorb relatively little signal. By contrast, heavy concrete, brick, and steel construction found in older buildings absorb and reflect much more power, resulting in high attenuation.

Multipath is a partial reflection of the signal from its intended path, resulting in it being received out of sync with the stronger non-reflected transmission, reducing link quality. Highly reflective surfaces such as water and glass, as well as foliage, are prone to multipath propagation even at shorter ranges.

Frequency Selection

Frequency impacts wireless performance in two ways:

- *Throughput*: Simply put, the higher the frequency, the higher the maximum theoretical throughput. High frequency radios may easily transmit 1 Gbps speeds, while lower frequencies are limited to 2-5 Mbps.
- *Penetration*: Due to their larger wavelength, lower frequencies are better able to penetrate and overcome partial or total obstacles. Low frequencies (900 MHz, 2.4 GHz, etc.) may function in non-line of sight (NLoS) applications, while 20 or 40 GHz high frequency radios may see performance degraded by rain or fog due to moisture in the air.

Because of this, users must carefully consider the maximum required throughput, obstacles in the wireless transmission path, how they may possibly be overcome, and how critical potential outages may be.

We discuss frequencies typically used in surveillance systems below.

2.4/5.8 GHz

These frequencies are unlicensed, free for use by anyone, and most often used in typical surveillance applications such as connecting cameras across a parking lot, between two buildings, etc. Throughput varies depending on transmission technology and number of radios (see MIMO, below) used, but is typically in the range of ~25-40 for single radios, and 150 or more for MIMO models.

However, these two bands are also used by 802.11 (a/b/g/n/ac) networks in use in homes and business, increasing the potential for interference. 5.8 Ghz was previously more common in surveillance as it was less crowded than the 2.4 band, but with 802.11n (and now 802.11ac) access points common in both home and commercial settings, its advantage has been greatly reduced.

2.4 GHz may be used in shorter or lower throughput non-line of sight applications, as it may penetrate obstacles such as light tree cover. However, 5.8 GHz generally requires line of sight.

Additionally, 2.4 and 5.8 GHz are less able to penetrate obstacles than lower frequencies, making line of sight (LOS) key when deploying radios in these bands. In professional video surveillance, 5.8Ghz is more frequently used than 2.4Ghz as it is relatively less crowded.

900 MHz

900 MHz is the most common non-line of sight frequency, and is most often used when cameras do not have a clear view of the base station, such as parks or other areas with foliage cover.

Its lower frequency band is better able to penetrate obstacles than 2.4 or 5.8 GHz radios. This penetration comes with a tradeoff, however, as 900 MHz wireless links typically have lower throughput than higher frequencies, historically about ~15-25 Mb/s. However, newer MIMO models have increased throughput significantly, with 100+ Mb/s now common.

The 900 MHz frequency band, like 2.4 and 5.8 GHz, is crowded and may experience interference issues, as it is commonly used by many consumer products, such as wireless phones and microwave ovens.

10+ GHz

Wireless radios above 5.8 GHz (10, 20, 60, 80 GHz, etc.) were historically uncommon in surveillance but have seen wider use in the past few years, due to their higher bandwidth capacity (often up to 1 Gb/s). However, with 802.11ac based MIMO radios now more common, this benefit has been somewhat reduced.

These frequencies are much more susceptible to interference due to environmental conditions such as rain, snow, and fog, making link budget planning and proper alignment critical. However, radios in these frequencies are less likely to see interference issues because few other devices operate in these ranges, unlike 900 MHz or 2.4/5.8 GHz.

Additionally, radios in these bands are much more expensive than typical 2.4/5.8 GHz models, typically starting close to $1,000 USD per radio, with $1,500-2,000 not uncommon.

Licensed Bands

Some frequencies of the wireless spectrum are reserved for public safety use. In the US, 4.9 GHz is regulated for this reason, and those entities (typically, but not always, government entities) wishing to deploy radios in this band must apply for use. Other governments may reserve different bands.

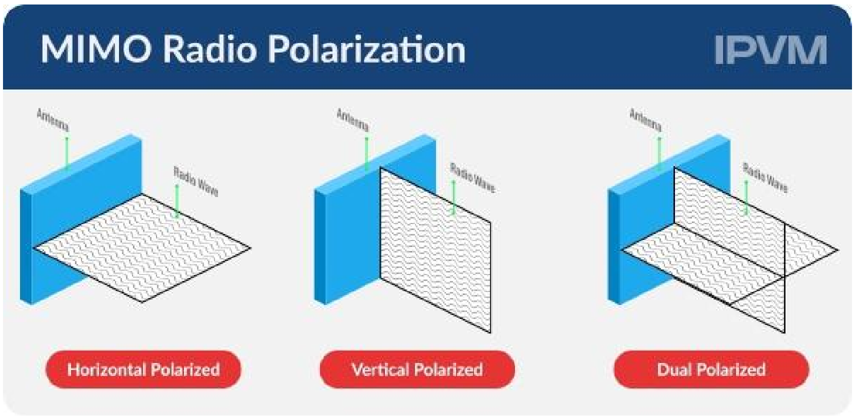
Because the government restricts who may use the 4.9 GHz band and on what channels in each area, interference issues are lessened compared to unlicensed frequencies. Because it is restricted to public safety use, it is most often seen in city surveillance, used by police and other emergency personnel.

TV White Space

A recent development in wireless, TV white space frequencies were first opened up to wireless network use in 2010. These radios use frequencies in the VHF/UHF range which were vacated in the switch from analog to digital broadcast TV. Since they use lower frequencies (between 54 and 806 MHz), white space radios are better able to penetrate obstacles, but throughput is lower than even 900 MHz, topping out at about 25 Mb/s in currently available product options.

MIMO Radios

MIMO, short for Multiple In Multiple Out, spreads radio signal across two or more paths to increase bandwidth and resistance to interference. MIMO radios may use two or more distinct antennas, or more commonly a dual-polarized antenna, which transmits both of these signals at once, with the beamwidths rotated 90 degrees. This image illustrates single versus dual-polarized antennas:



Bandwidth Planning

Environmental and site conditions may impact bandwidth significantly, especially as frequencies increase. 5.8 GHz frequencies and below are generally not affected by any but the most severe weather, such as heavy snow or torrential rain. Frequencies above this, however, may be impacted greatly, and thus should not be used for critical surveillance links. Aside from weather, slight changes in site conditions, such as foliage growing into the path of transmission, or antennas shifting slightly may cause intermittent issues, decreased bandwidth, or complete loss of link.

Manufacturer Bandwidth Claims

Be careful about manufacturer bandwidth claims. As a general rule of thumb, discount specified bandwidth levels by 50% to 75% when estimating potential for real world surveillance use. The good news is that even with such caution, wireless bandwidth even for a single HD camera (~2-8 Mb/s) is generally easy to deliver on a dedicated PtP link. However, as wireless video systems get bigger and more complex, more careful estimation and testing becomes critical.

Transmission Range

There are no hard and fast rules for transmission range in wireless networks. Distances are affected by issues such as obstructions, frequency used, transmission power, and antenna gain.

In typical installations where line of sight is possible, such as parking lots, distance is not much of a challenge when standard antennas in PtP or PtMP configurations.

However, while multi-mile wireless links are easily possible with the right equipment, many users will find the calculations required in these scenarios challenging, and novice users should seek assistance from the manufacturer or experienced integrators.

Additionally, the longer the link, the more precise antenna alignment must be, making installation more difficult. Multi-mile links even must take the curvature of the earth into account, as it may reflect or absorb signal at long ranges, discussed above.

Wireless Products for Video Surveillance

Since cameras rarely have built-in wireless, typically surveillance systems will use specialist wireless equipment instead of trying to connect to a home or SMB wireless router.

Most wireless surveillance users typically deploy PTP or PtMP systems, generally with lower cost systems (Ubiquiti is the most common). For more on wireless product preferences, see: Favorite Wireless Video Surveillance Manufacturers.

In the 2000s, there was a lot of money and interest in mesh networking but the high cost ($3,000+ per link was common) and complexity has relegated that mostly to high-end, complicated projects.

Maintenance

Because wireless links are sensitive to fluctuations in site conditions, routine maintenance is a key concern in any deployment. Antenna alignment should be checked, connectors should be checked for corrosion, foliage in the path of the link should be trimmed, and more. We examine these issues in-depth in our Wireless Surveillance Recommendations.

Power Requirements A major obstruction to installing wireless-connected cameras is determining the best available power source. The power draw for a typical radio and camera will be low (less than 60 watts). Finding continuous, clean supply near the required location is the primary obstacle. If no power source exists, power draw will need to be taking into account for Solar or Battery powered systems.**Electrical License Required** Always consult a licensed electrician when installing a new or using an existing power source. If you or the client do not have one on staff, you will need to account for the additional cost of subcontracting one. This is important as the supply voltages can cause injury or death to inexperienced technicians, or damage expensive equipment. A licensed electrician will also ensure you get the correct information about existing power sources (do not automatically rely on the client's maintenance staff). The most common power sources that are used:

- Utility Power
- Solar
- Battery

Utility Power

Powering wireless radios and cameras with a standard 110-120VAC @ 60 Hz (or 220-240VAC @ 50Hz) utility-connected outlet or hardwired power supply is the easiest solution.

For installation of a camera on a building that doesn't have existing network connectivity, power can be pulled from a nearby electrical junction box, or even by extended off an existing circuit. This can be common on maintenance sheds, Sports Fields, and remote vehicle garage installations.

Installing cameras on lighting poles may also use the electrical power that is feeding the pole. This will depend on a few factors:

- Is the power at the pole centrally switched? In many commercial situations, multiple lighting poles are controlled by a building located timer, or photo-eye, which turns the power off to the lights during the day.
- Is the power compatible with surveillance equipment? Some lighting poles run on higher 3-phase voltages like 277 or 480 volts, so that can prevent you from using that power without a step-down transformer.

IPVM has a Guide on Using Switched Power for surveillance systems.

Solar Power

The viability of solar power for wireless video surveillance will depend on the region you are installing. The US Government National Renewable Energy Lab produces a map that shows the energy available in all 50 states.

Other resources are available for estimating the solar energy available, like the Global Solar Atlas. IPVM has a Guide for Solar Surveillance installation.

You will then need to calculate the energy required for your system, and see if a combination of solar panels with battery backup will work where you are installing.

Another factor to consider when installing a solar powered system is the additional weight and aesthetics of both the solar panel and the associated control boards and battery storage units.

Solar Power systems will result in higher recurring costs of maintaining the solar panels and battery backup systems.

Battery Power

Battery backup power is part of any Solar Powered system and is added to Switched Power installations when the power supply is unreliable. Maintenance of the batteries is critical to the performance of any system and will add recurring cost.

Cameras like Ezviz, Arlo or Blink that are completely battery-powered are consumer-focused products, and integration with a VMS platform or ONVIF support is rare. Manufacturers claim a battery life of 4-9 months. This could be shortened to a few weeks depending on the amount of activity monitored. Cameras will be taken offline while replacing the batteries in some units. Cameras with rechargeable batteries may need to be uninstalled while charging offline.

Test Your Knowledge

Take this 9 question quiz now